



Vendor: HP

Exam Code: HPE6-A07

Exam Name: Aruba Certified ClearPass Associate 6.5

Version: DEMO

QUESTION 1

Based on the self-registration customization, what is the expected outcome?

Customize Guest Registration	
NAS Login Options controlling logging into a NAS for self-registered guests.	
Enabled:	<input checked="" type="checkbox"/> Enable guest login to a Network Access Server
* Vendor Settings:	Aruba Networks Select a predefined group of settings suitable for standard network configurations.
Login Method:	Controller-initiated – Guest browser performs HTTP form submit Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive p
IP 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:	<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 mac The address above will be used whenever the parameter is not available or fails the requirements
Default Destination Options for controlling the destination clients will redirect to after login.	
Default URL:	<input type="text"/> Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.
Override Destination:	<input type="checkbox"/> Force default destination for all clients If selected, the client's default destination will be overridden regardless of its value.
<input type="button" value="Save Changes"/> <input type="button" value="Save and Continue"/>	

- When the user connects to an ArubaNAD device, the user will be redirected to this self-registration page.
- When the user completes the self-registration form, a NAS login request will be sent from the client to ClearPass alternate domain at securelogin.arubanetworks.com.
- When the user browses to securelogin.arubanetworks.com, the user will be redirected to the self-registration page.
- User credentials will be sent to the NAD device when the user clicks the login button on the self-registration receipt page.
- When the user clicks the register button on the self-registration page, user credentials will be sent to the NAD.

Answer: B

QUESTION 2

Refer to the exhibit. A user connects to an Aruba Access Point wireless SSID named "secure-corporate" and performs an 802.1X authentication with ClearPass as the authentication server.

Configuration>>Services>>Reorder

Reorder Services

Order	Name
1	[Policy Manager Admin Network Service]
2	pod8wired
3	pod8-mac auth
4	pod8wireless

Service Rule

```
( (Radius:IETF:NAS-Port-Type EQUALS Ethernet (15))
AND (Radius:IETF:Service-Type BELONGS_TO Login-User (1), Framed-User (2), Authenticate-Only (8)) )
AND (Connection:Protocol EQUALS RADIUS)
```

Service Rule

```
( (Radius:IETF:NAS-Port-Type BELONGS_TO Ethernet (15), Wireless-802.11 (19))
AND (Radius:IETF:Service-Type BELONGS_TO Login-User (1), Call-Check (10))
AND (Connection:Client-Mac-Address EQUALS %{Radius:IETF:User-Name})) )
AND (Connection:Protocol EQUALS RADIUS)
```

Service Rule

```
( (Radius:IETF:NAS-Port-Type EQUALS Wireless-802.11 (19))
AND (Radius:IETF:Service-Type BELONGS_TO Login-User (1), Framed-User (2), Authenticate-Only (8))
AND (Radius:Aruba:Aruba-Location-Id EXISTS )
AND (Radius:Aruba:Aruba-Essid-Name EXISTS ) )
AND (Connection:Protocol EQUALS RADIUS)
```

Based on this service configuration, which service will be triggered?

- A. pod8-mac auth
- B. Noservice will be triggered
- C. pod8wireless
- D. [Policy Manager Admin Network Service]
- E. pod8wired

Answer: A

QUESTION 3

When enforcement action is used in ClearPass to bounce a client?

- A. Webpage redirect
- B. ACL
- C. VLAN attribute
- D. RADIUS VSA
- E. RADIUS CoA

Answer: E

Explanation:

In the Profiler tab, change the RADIUS CoA Action to "[Cisco -Bounce-Host-Port]". Make sure your switch is configured for this.

QUESTION 4

What is the purpose of the pre-auth check during guest authentication?

- A. for the NAD device to do an internal authentication check before sending the credentials to ClearPass
- B. for the NAD device to check that ClearPass is active before sending it the RADIUS request
- C. for ClearPass to do an internal authentication check before the NAS login happens
- D. for the client device to do an internal sanity check before the NAS login occurs
- E. for the client device to check that ClearPass is active before sending it the credentials

Answer: C

Explanation:

The way NAS devices like wireless controllers do authentication on external captive portals only allows standard reject message handling like "authentication failed". The pre auth check allows CPPM to provide advanced error handling of a reject like "your time limit has been reached" before a user logs in. It is to do an end run around limited error handling of NAS devices on external captive portals.

<https://community.arubanetworks.com/t5/Security/why-use-pre-auth-check/m-p/93254>

QUESTION 5

Which statement most accurately describes how users with Active Directory credentials authenticate with ClearPass when Active Directory is used as an authentication source for an 802.1x service in ClearPass?

- A. A Kerberos request is sent from the Network Access Device to ClearPass which initiates a RADIUS request to the AD server.
- B. A RADIUS request is sent from the Network Access Device to the AD server which communicates with ClearPass.
- C. An LDAP request is sent from the Network Access Device to the AD server which communicates with ClearPass.
- D. An LDAP request is sent from the Network Access Device to ClearPass which initiates a RADIUS request to the AD server.
- E. A RADIUS request is sent from the Network Access Device to the ClearPass which communicates with the AD server.

Answer: C

Explanation:

http://www.arubanetworks.com/techdocs/ClearPass/Aruba_DeployGd_HTML/Content/3%20Active%20Directory/AD_auth_source_adding.htm

QUESTION 6

How is ClearPass enabled to perform DHCP profiling for devices in a network?

- A. by enabling a port mirror on the network access device to mirror all user traffic to ClearPass
- B. by enabling DHCP relay on our network access devices so DHCP requests are forwarded to ClearPass
- C. by enabling the 'DHCP ignore' feature on network access devices
- D. by configuring ClearPass as a secondary DHCP server on the client
- E. by enabling profiling on ClearPass; configuration of the network access devices is not necessary

Answer: B

Explanation:

<https://community.arubanetworks.com/aruba/attachments/aruba/ForoenEspanol/653/1/ClearPass%20Profiling%20TechNote.pdf>

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad.**
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER
NETWORKS



EMC²
where information lives®

10% Discount Coupon Code: ASTR14