# HPE6-A79$^{Q\&As}$

Aruba Certified Mobility Expert Written Exam

## Pass HP HPE6-A79 Exam with 100% Guarantee

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

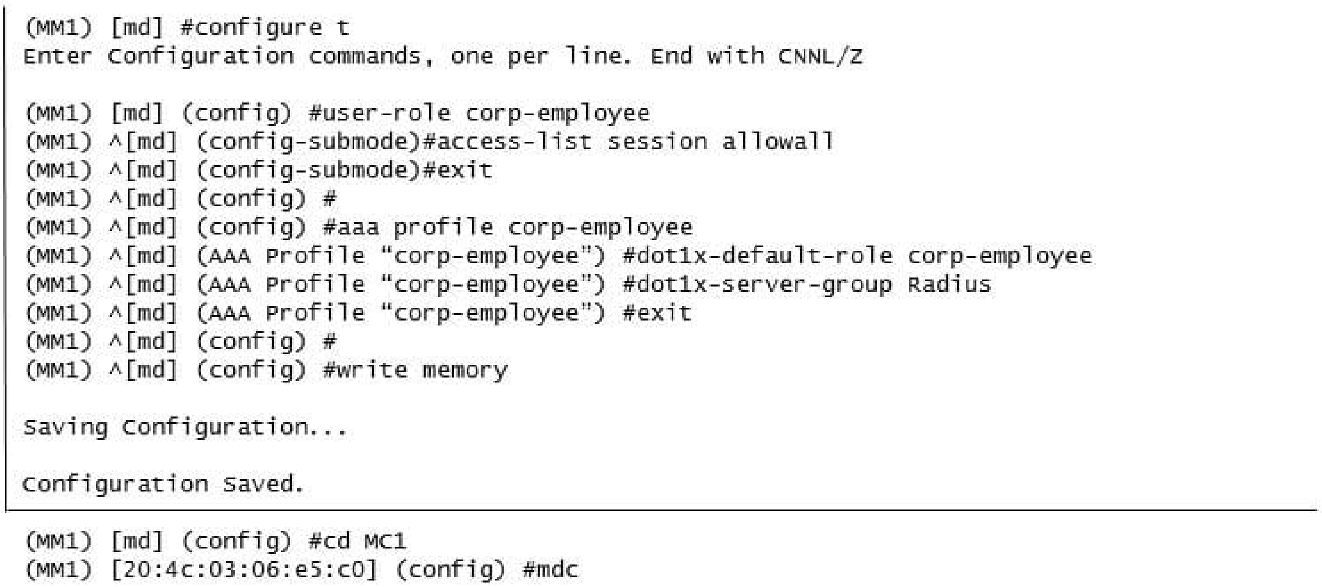
**https://www.geekcert.com/hpe6-a79.html**

100% Passing Guarantee
100% Money Back Assurance

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

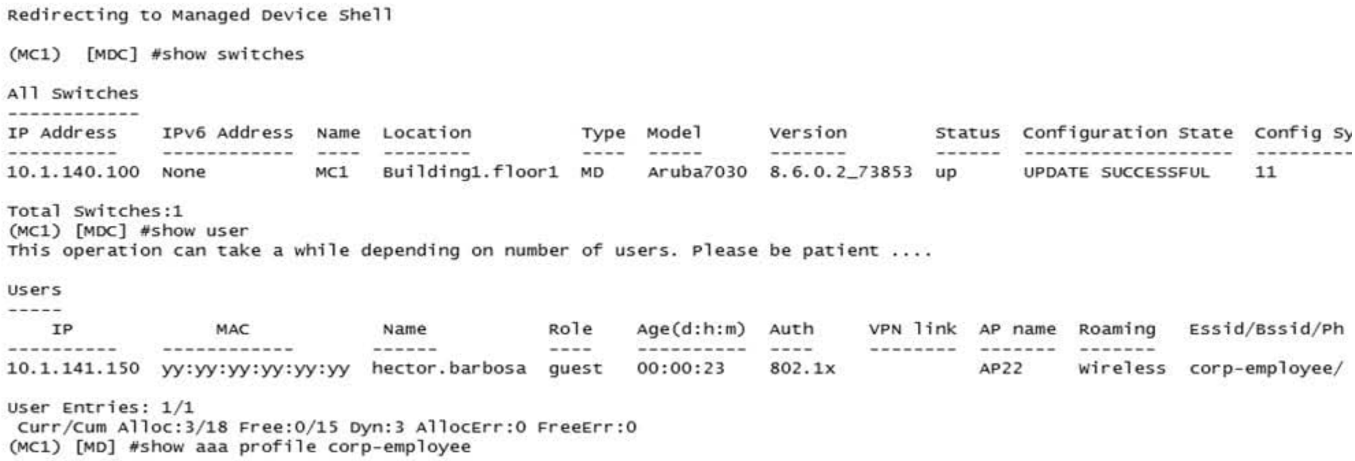
**QUESTION 1**

Refer to the exhibits.

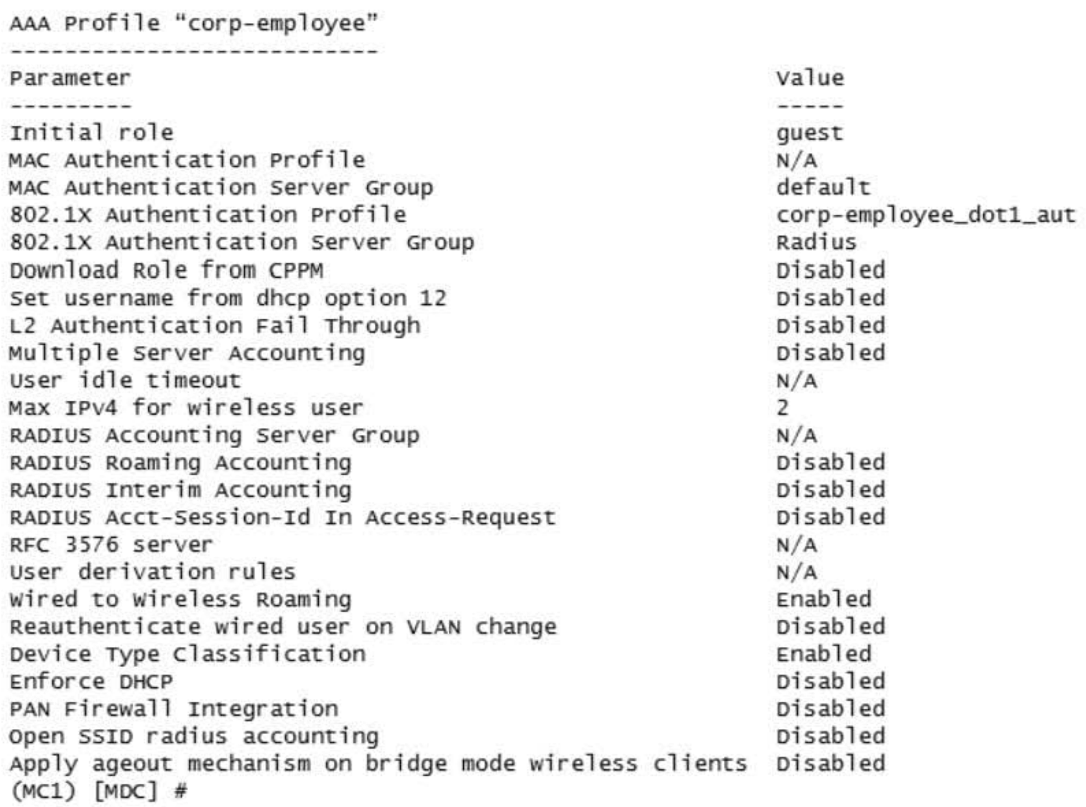


```
(MM1) [md] #configure t
Enter Configuration commands, one per line. End with CNNL/Z

(MM1) [md] (config) #user-role corp-employee
(MM1) ^[md] (config-submode)#access-list session allowall
(MM1) ^[md] (config-submode)#exit
(MM1) ^[md] (config) #
(MM1) ^[md] (config) #aaa profile corp-employee
(MM1) ^[md] (AAA Profile “corp-employee”) #dot1x-default-role corp-employee
(MM1) ^[md] (AAA Profile “corp-employee”) #dot1x-server-group Radius
(MM1) ^[md] (AAA Profile “corp-employee”) #exit
(MM1) ^[md] (config) #
(MM1) ^[md] (config) #write memory

Saving Configuration...

Configuration Saved.
```

```
(MM1) [md] (config) #cd MC1
(MM1) [20:4c:03:06:e5:c0] (config) #mdc
```



```
Redirecting to Managed Device Shell

(MC1)  [MDC] #show switches

All Switches
------------
IP Address    IPv6 Address  Name  Location          Type  Model      Version        Status  Configuration State  Config Sy
----------    ------------  ----  --------          ----  -----      -------        ------  -------------------  ---------
10.1.140.100  None          MC1   Building1.floor1  MD    Aruba7030  8.6.0.2_73853  up      UPDATE SUCCESSFUL    11

Total Switches:1
(MC1) [MDC] #show user
This operation can take a while depending on number of users. Please be patient ....

Users
-----
    IP             MAC            Name           Role    Age(d:h:m)  Auth     VPN link  AP name  Roaming   Essid/Bssid/Ph
----------    ------------     ------          ----    ----------  ----     --------  -------  -------
10.1.141.150  yy:yy:yy:yy:yy:yy  hector.barbosa  guest   00:00:23    802.1x             AP22     wireless  corp-employee/

User Entries: 1/1
 Curr/Cum Alloc:3/18 Free:0/15 Dyn:3 AllocErr:0 FreeErr:0
(MC1) [MD] #show aaa profile corp-employee
```



```
AAA Profile “corp-employee”
---------------------------
Parameter                                               Value
---------                                               -----
Initial role                                            guest
MAC Authentication Profile                              N/A
MAC Authentication Server Group                         default
802.1X Authentication Profile                           corp-employee_dot1_aut
802.1X Authentication Server Group                      Radius
Download Role from CPPM                                 Disabled
Set username from dhcp option 12                        Disabled
L2 Authentication Fail Through                          Disabled
Multiple Server Accounting                              Disabled
User idle timeout                                       N/A
Max IPv4 for wireless user                              2
RADIUS Accounting Server Group                          N/A
RADIUS Roaming Accounting                               Disabled
RADIUS Interim Accounting                               Disabled
RADIUS Acct-Session-Id In Access-Request                Disabled
RFC 3576 server                                         N/A
User derivation rules                                   N/A
Wired to Wireless Roaming                               Enabled
Reauthenticate wired user on VLAN change                Disabled
Device Type Classification                              Enabled
Enforce DHCP                                            Disabled
PAN Firewall Integration                                Disabled
Open SSID radius accounting                             Disabled
Apply ageout mechanism on bridge mode wireless clients  Disabled
(MC1) [MDC] #
```

A network administrator has fully deployed a WPA3 based WLAN with 802.1X authentication. Later he defined corp-employee as the default user-role for the 802.1X authentication method in the aaa profile. When testing the setup he realizes the client gets the "guest" role.

What is the reason "corp-employee" user role was not assigned?

A. The administrator forgot to map a dot1x profile to the corp-employee aaa profile.

B. The administrator forgot to enable PEFNG feature set on the Mobility Master.

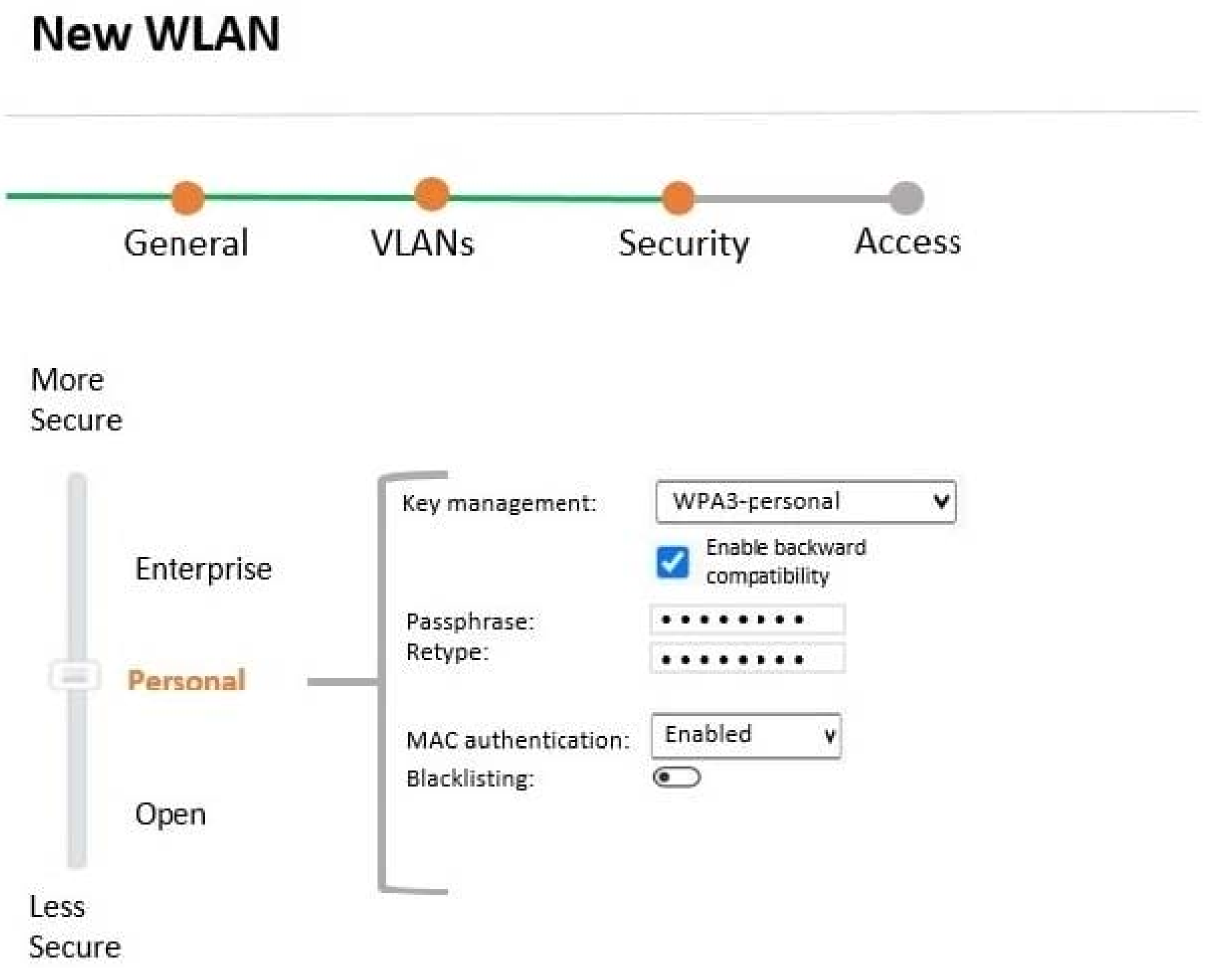
C. MC 1 has not received the configuration from the mobility master yet.

D. The Mobility Master lacks MM-VA licenses; therefore, it shares partial configuration only.

Correct Answer: C

**QUESTION 2**

Refer to the exhibit: A company acquires ten barcode scanners to run inventory tasks. These WiFi devices support WPA2-PSK security only. The network administrator deploys a WLAN named scanners using the configuration shown in the exhibit. What must the network administrator do next to ensure that the scanner devices successfully connect to their SSID?



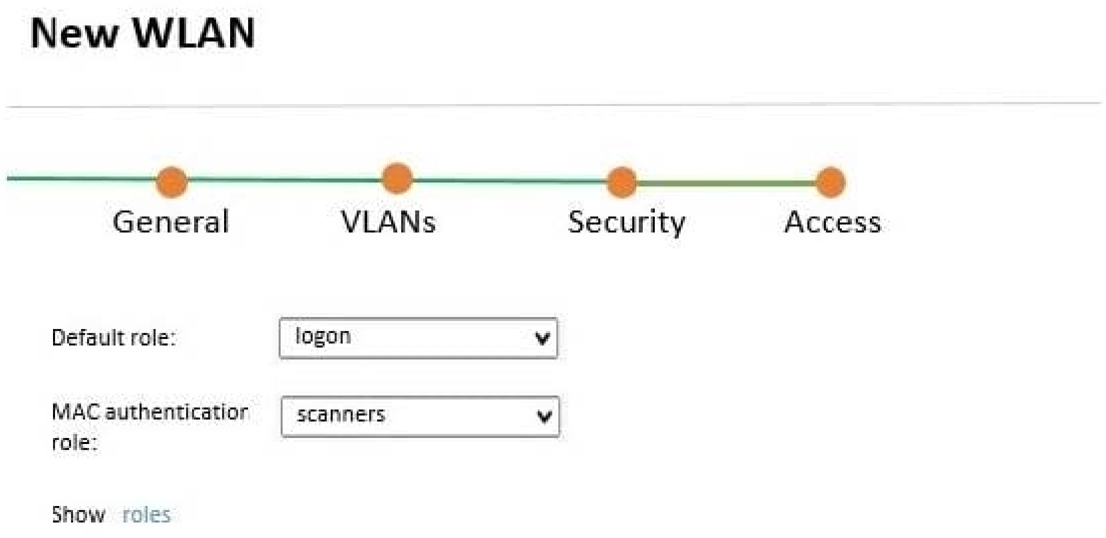
New WLAN

Key management: WPA3-personal

☑ Enable backward compatibility

Passphrase: •••••••••
Retype: •••••••••

MAC authentication: Enabled
Blacklisting: ○



New WLAN

Default role: logon

MAC authentication role: scanners

Show roles

A. Set internal as the MAC authentication server group.

B. Add scanner MAC addresses in user derivation rules.

C. Enable L2 Authentication Fail Through.

D. Add scanner MAC addresses in the internal database.

Correct Answer: D

**QUESTION 3**

A network administrator is in charge of a Mobility Master (MM) ?Mobility Controller (MC) based network security. Recently the Air Monitors detected a Rogue AP in the network and the administrator wants to enable "Tarpit" based wireless containment.

What profile must the administrator enable "tarpit" wireless containment on?

A. IDS Unauthorized device profile

B. IDS profile

C. IDS General profile

D. IDS DOS profile

Correct Answer: A

**QUESTION 4**

A network administrator assists with the migration of a WLAN from a third-party vendor to Aruba in different locations throughout the country. In order to manage the solution from a central point, the network administrator decides to deploy redundant Mobility Masters (MMs) in a datacenter that are reachable through the Internet.

Since not all locations own public IP addresses, the security team is not able to configure strict firewall polices at the datacenter without disrupting some MM to Mobility Controller (MC) communications. They are also concerned about exposing the MMs to unauthorized inbound connection attempts.

What should the network administrator do to ensure the solution is functional and secure?

A. Deploy an MC at the datacenter as a VPN concentrator.

B. Block all inbound connections, and instruct the MM to initiate the connection to the MCs.

C. Block all ports to the MMs except UDP 500 and 4500.

D. Install a PEFV license, and configure firewall policies that protect the MM.

Correct Answer: C

**QUESTION 5**

A company with 50 small coffee shops in a single country requires a single mobility solution that solves connectivity needs at both the main office and branch locations. Coffee shops must be provisioned with local WiFi internet access for customers.

The shops must also have a private WLAN that offers communication to resources at the main office to upload sales, request supplies through a computer system, and make phone calls if needed. In order to simplify network operations, network devices at the coffee shops should be cloud managed.

Which technologies best meet the company needs at the lowest cost?

A. IAP VPN

B. SD-Branch

C. Activate with RAPs

D. BOC with CAPs

Correct Answer: B