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:

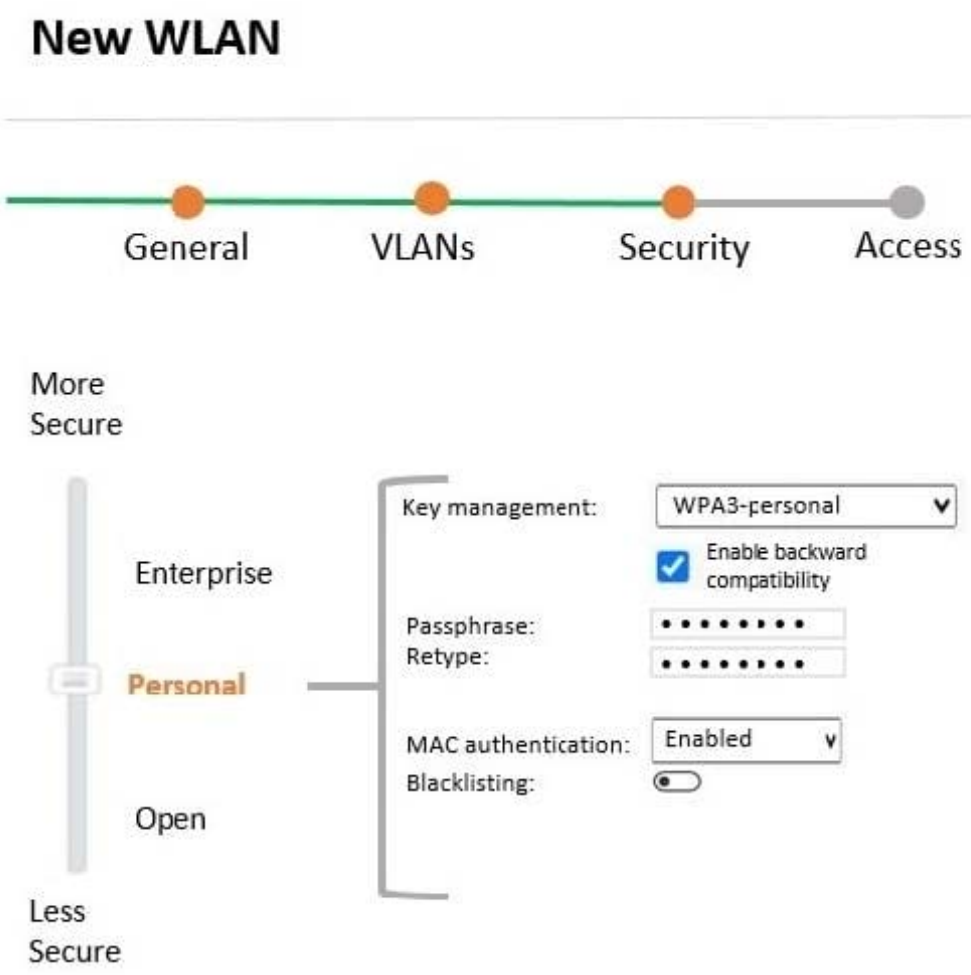
https://www.pass4itsure.com/hpe6-a79.html

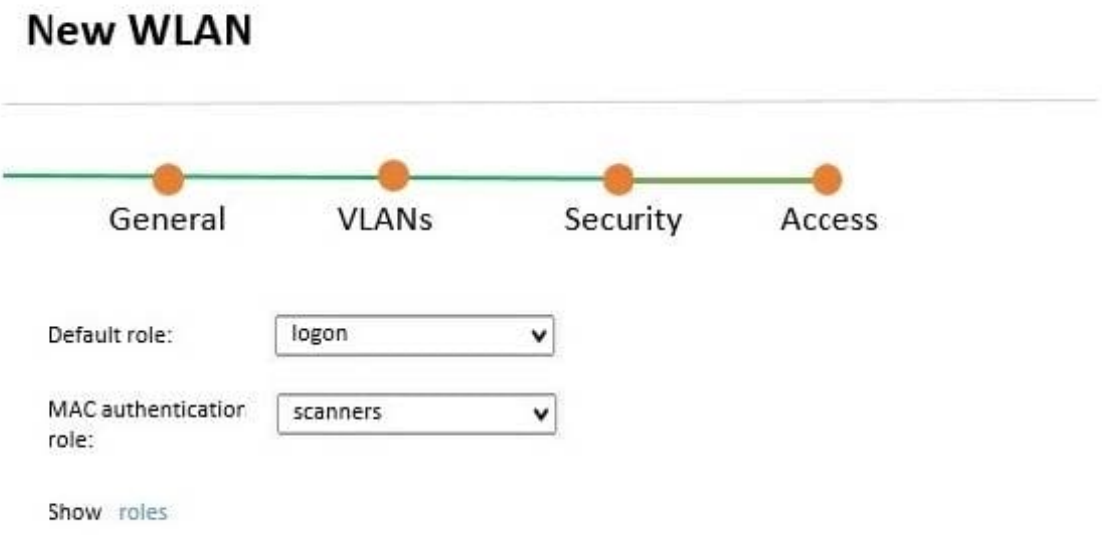
100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Refer to the 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?





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 2

Refer to the exhibit.

```
(MM)[mynode] #show airmatch event all-events ap-name AP2
```

Band	Event Type	Radio	Timestamp	Chan	CBW	New Chan	New CBW	APName
5GHz	RADAR_DETECT	xx:xx:xx:xx:xx:xx	2018-07-25_07:50:05	100	80MHz	149	80MHz	AP2
5GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	2018-07-24_07:48:42	124	80MHz	100	80MHz	AP2
5GHz	RADAR_DETECT	xx:xx:xx:xx:xx:xx	2018-07-23_16:44:36	100	80MHz	124	80MHz	AP2
5GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	2018-07-20_19:12:34	157	80MHz	100	80MHz	AP2
5GHz	RADAR_DETECT	xx:xx:xx:xx:xx:xx	2018-07-20_10:02:30	100	80MHz	157	80MHz	AP2
5GHz	RADAR_DETECT	xx:xx:xx:xx:xx:xx	2018-07-20_08:34:31	56	80MHz	100	80MHz	AP2
2GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	2018-07-25_08:31:31	11	20MHz	6	20MHz	AP2
2GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	2018-07-25_08:31:31	6	20MHz	1	20MHz	AP2
2GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	2018-07-24_07:46:34	1	20MHz	11	20MHz	AP2
2GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	2018-07-24_07:46:33	6	20MHz	1	20MHz	AP2
2GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	2018-07-23_15:13:15	11	20MHz	6	20MHz	AP2
2GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	2018-07-23_15:12:12	1	20MHz	11	20MHz	AP2
2GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	2018-07-20_08:07:27	11	20MHz	1	20MHz	AP2
2GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	2018-07-20_08:07:26	6	20MHz	11	20MHz	AP2
2GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	2018-07-19_19:22:45	1	20MHz	6	20MHz	AP2
2GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	2018-07-19_19:22:44	11	20MHz	1	20MHz	AP2
2GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	2018-07-19_10:45:23	1	20MHz	11	20MHz	AP2

A network administrator deploys a Mobility Master (MM) - Mobility Controller (MC) network with Aps in different locations. Users in one of the locations report that the WiFi network works fine for several hours, and then they are suddenly

disconnected. This symptom may happen at any time, up to three times every day, and lasts no more than two minutes.

After some research, the network administrator logs into the MM and reviews the output shown in the exhibit.

Based on this information, what is the most likely reason users get disconnected?

A. Adaptive Radio Management is reacting to RF events.

B. AirMatch is applying a scheduled optimization solution.

C. Users in the 2.4 GHz band are being affected by high interference.

D. AirMatch is reacting to non-scheduled RF events.

Correct Answer: C

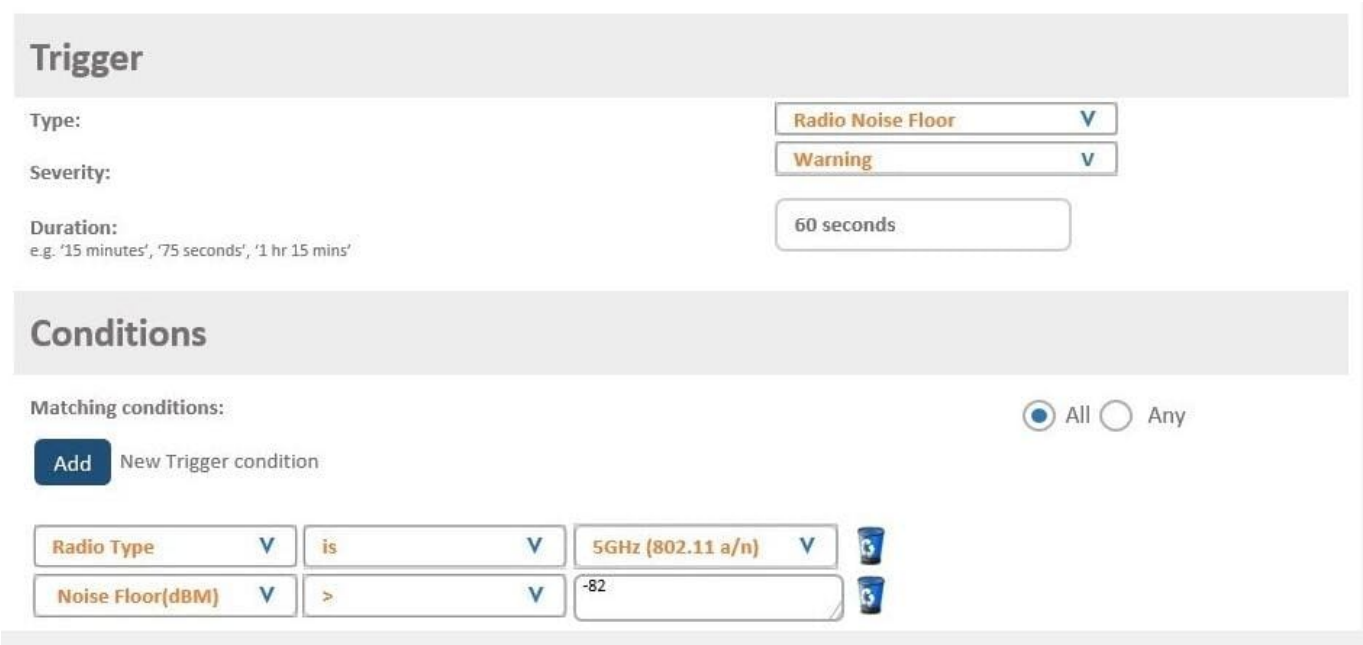
QUESTION 3

HOTSPOT

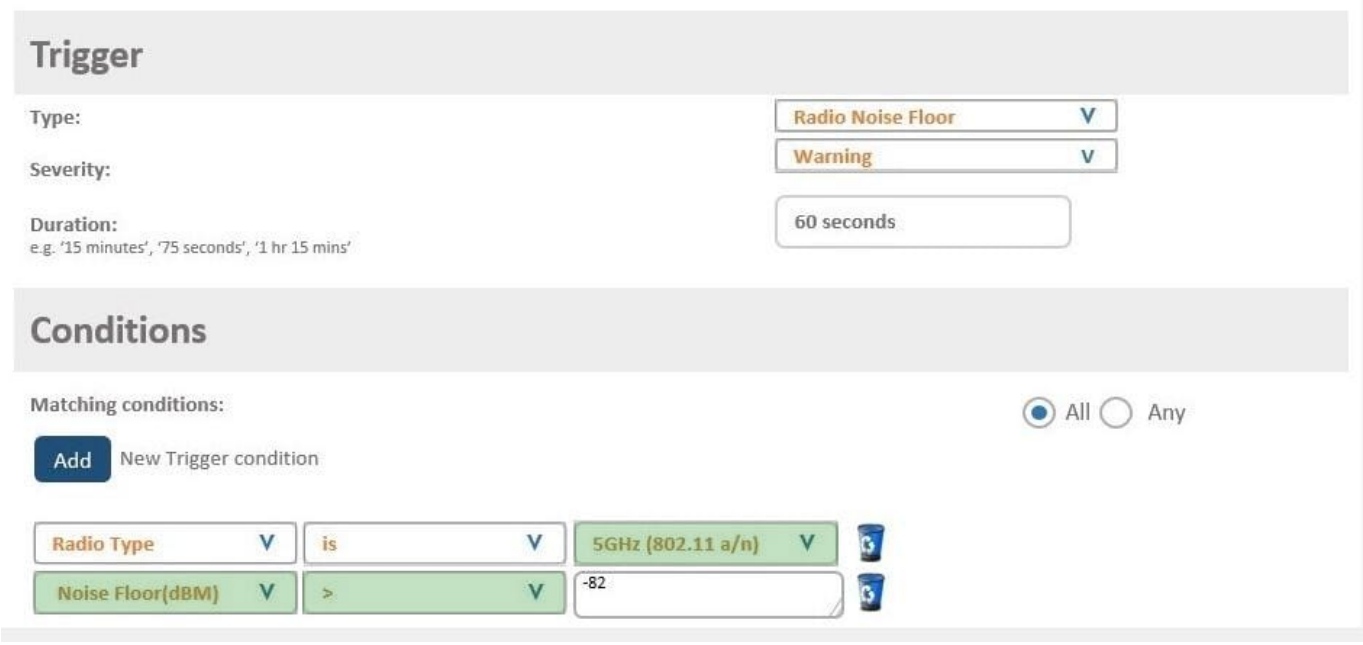
A network administrator wants to receive a warning level alarm every time the noise floor rises above -82 dBm on any of the AP radios.

Which alarm definition must the network administrator create to accomplish this?

Hot Area:



Correct Answer:



QUESTION 4

Refer to the exhibits. Exhibit 1

```
(MC2) [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/Phy                          Profile          Forward mode  Type
Host Name   User Type
---------   ----------        -----  ----    ---------  ----    -------  -------  -------  ---------------                          -------          ------------  -----
---------   --------
10.1.141.150  xx:xx:xx:xx:xx:xx  it    guest   00:00:48   802.1x           AP22     Wireless Corp-employee/yy:yy:yy:yy:yy:yy/a-VHT    Corp-Network     tunnel        Win 10
            WIRELESS

User Entries: 1/1
  Curr/Cum Alloc:3/39  Free:0/36 Dyn:3 AllocErr:0 FreeErr:0
(MC2) [MDC] #
(MC2) [MDC] #show user ip 10.1.141.150 | include Role
This operation can take a while depending on number of users. Please be patient ....
Role: guest (how: ROLE_DEPRIVATION_DOTIX), ACL: 7/0
Role Deprivation: ROLE_DEPRIVATION_DOTIX
(MC2) [MDC] #
```

Exhibit 2

```
(MC2) [MDC] #show log security 300

Jul 4 17:32:15 :124004: <3553> <DBUG> |authmgr| Select server method=802.1x, user=it, essid=Corp-employee, server-group=Corp-Network, last_srv <>
Jul 4 17:32:15 :124038: <3553> <INFO> |authmgr| Reused server ClearPass.23 for method=802.1x; user=it, essid=Corp-employee, domain=<>, server-group=Corp-Network
Jul 4 17:32:15 :124004: <3553> <DBUG> |authmgr| aal_auth_raw (1402) (INC) : cs_reqs 1, s ClearPass.23 type 2 inservice 1 markedD 0
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:152] Radius authenticate raw using server ClearPass.23
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_request.c:67] Add Request: id=22, server=ClearPass.23, IP=10.254.1.23, server-group=Corp-Network, fd=64
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2367] Sending radius request to ClearPass.23:10.254.1.23:1812 id:22, len:265
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] User-Name: it
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-IP-Address: 10.254.10.214
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-Port-Id: 0
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-Identifier: 10.1.140.101
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-Port-Type: Wireless-IEEE802.11
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Calling-Station-Id: 814F0C517FS6
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Called-Station-Id: 193D1247D881
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Service-Type: Framed-User
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Framed-MTU: 1100
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] EAP-Message: \002\011
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] State: AFMAzwACACAG9glAfvORnQM2udKK13smu/I2DA==
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-Essid-Name: Corp-employee
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-Location-Id: AP22
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-AP-Group: CAMPUS
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-Device-Type: Win 10
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Message-Auth: d\466\487\328\679wvx\487"\642z\812P\540\115
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:95] Find Request: id=22, server=(null), IP=10.254.1.23, server-group=(null) fd=64
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:104] Current entry: server=(null), IP=10.254.1.23, server-group=(null) fd=64
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:48] Del Request: id=22, server=ClearPass.23, IP=10.254.1.23, server-group=Corp-Network, fd=64
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1228] Authentication Successful
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1230] RADIUS RESPONSE ATTRIBUTES:
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1245] Filter-Id: it-role
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1245] (Microsoft) MS-MPPE-Recv-Key: \555\554\801\861\353[1*;\877g$\574\856u\302\215\237^"\857\2257\843F\4265<\2
57R\487\016\547$\109\146\506\605:\384\603\200\716R\508\666\032\750\413\480
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1245] (Microsoft) MS-MPPE-Send-Key: \456\311\781\648\789I\549\K\950\345\366F\276\789.7\642e\917\331\983\389\11
5\7764jD@7\763T\649\865/\339\992\587\756x\456[\487\4937u\415\308l
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1245] EAP-Message: \003\011
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1245] Message-Auth: \789,\156\734I\111\555\871\456t\478\119;752{\723\490
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1245] User-Name: it
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1245] Class: \514\678\820)\430\513C\749\0548#\648\700\438"\112\754\261
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1245] PW_RADIUS_ID: \026
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1245] Rad-Length: 231
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1245] PW_RADIUS_CODE: \002
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1245] PW_RAD_AUTHENTICATOR: \447rV\623\765/)F\894t\384\065\413\395\243\084
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| Authentication result= Authentication Successful(0), method=802.1x, server=ClearPass.23, user=xx:xx:xx:xx:xx:xx
```

A network administrator integrates a current Mobility Master (MM) - Mobility Controller (MC) deployment with a RADIUS server to authenticate a wireless user, the network administrator realizes that the client machine is not failing into the it_department role, as shown the exhibits.

Which configuration is required to map the users into the proper role, based on standard attributes returned by the RADIUS server in the Access Accept message?

A. aaa server-group Corp-Network set role condition Filter-Id equals it-role set-value it_department

B. aaa server-group Corp-employee set role condition Filter-Id value-of

C. aaa server-group Corp-employee set role condition Filter-Id equals it-role set-value it_department

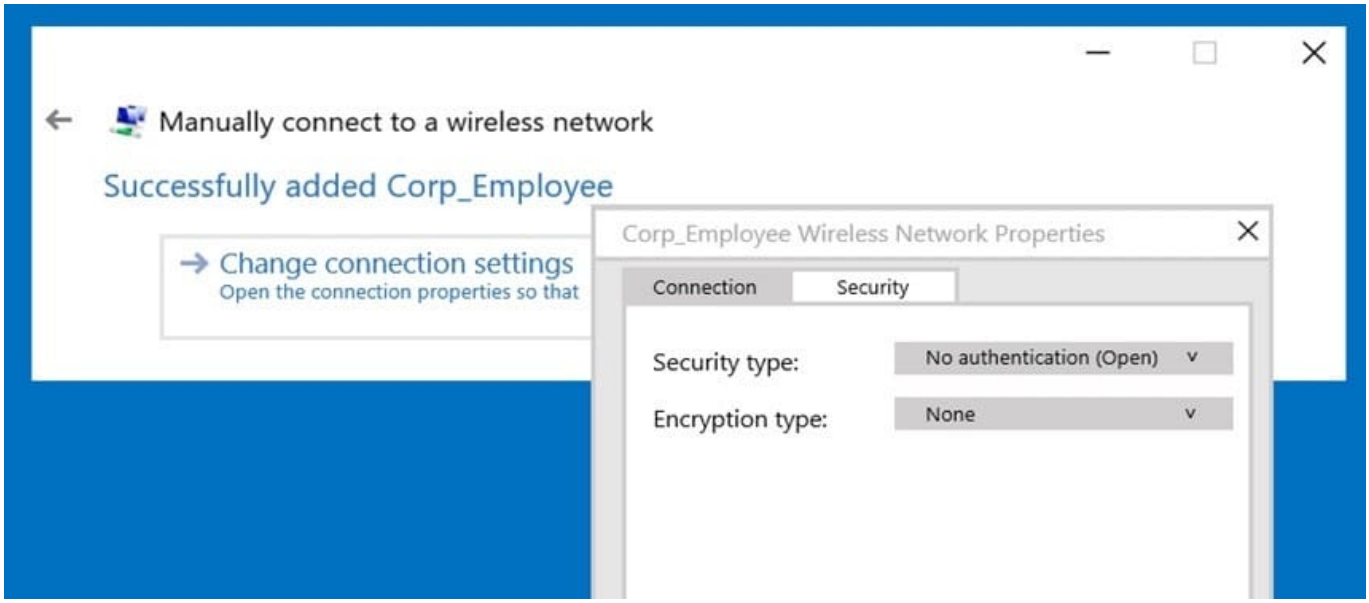
D. aaa server-group ClearPass set role condition Filter-Id equals it_department set-value it-role

E. aaa server-group Corp-Network set role condition Filter-Id equals it_department set-value it-role

Correct Answer: C

QUESTION 5

Refer to the exhibit.



A network administrator wants to configure an 802.1x supplicant for a wireless network that includes the following:

AES encryption EAP-MSCHAP v2-based user and machine authentication Validation of server certificate in Microsoft Windows 10

The network administrator creates a WLAN profile and selects the change connection settings option. Then the network administrator changes the security type to Microsoft: Protected EAP (PEAP), and enables user and machine authentication under Additional Settings.

What must the network administrator do next to accomplish the task?

A. Change default RC4 encryption for AES.

B. Enable user authentication under Settings

C. Change the security type to Microsoft: Smart Card or other certificate.

D. Enable server certificate validation under Settings.

Correct Answer: C