



300-430^{Q&As}

Implementing Cisco Enterprise Wireless Networks (ENWLSI)

Pass Cisco 300-430 Exam with 100% Guarantee

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

<https://www.passapply.com/300-430.html>

100% Passing Guarantee
100% Money Back Assurance

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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

An engineer has many different WLANs on a WLC but does not want to broadcast them to every AP in the building. Which group must be configured on the WLC to allow different WLANs on the different APs without creating new interfaces?

- A. ACL
- B. interface group
- C. mobility group
- D. AP group

Correct Answer: D

QUESTION 2

Refer to the exhibit.



```
(Cisco Controller) >  
(Cisco Controller) >*EAP Framework: Jan 21 23:55:43.569: eap_fast.c-EVENT: New context (EAP handle = c4000000)  
*EAP Framework: Jan 21 23:55:43.569: eap_fast.c-EVENT: Allocated new EAP-FAST context (handle = 37000000)  
*EAP Framework: Jan 21 23:55:43.569: eap_fast_auth.c-AUTH-EVENT: Process Response (EAP handle = c4000000)  
*EAP Framework: Jan 21 23:55:43.569: eap_fast_auth.c-AUTH-EVENT: Received Identity  
*EAP Framework: Jan 21 23:55:43.569: eap_fast_tlv.c-AUTH-EVENT: Adding PAC A-ID TLV (436973636f00000000000000000000000000000000)  
*EAP Framework: Jan 21 23:55:43.569: eap_fast_auth.c-AUTH-EVENT: Sending Start  
*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b  
*EAP Framework: Jan 21 23:55:43.586: eap_fast_auth.c-AUTH-EVENT: Process Response (EAP handle = c4000000)  
*EAP Framework: Jan 21 23:55:43.586: eap_fast_auth.c-AUTH-EVENT: Received TLS record type: Handshake in state: Start  
*EAP Framework: Jan 21 23:55:43.586: eap_fast_auth.c-AUTH-EVENT: Reading Client Hello handshake  
*EAP Framework: Jan 21 23:55:43.586: eap_fast_auth.c-AUTH-EVENT: Ignoring unknown ext rec type: 10  
*EAP Framework: Jan 21 23:55:43.586: eap_fast_auth.c-AUTH-EVENT: Ignoring unknown ext rec type: 11  
*EAP Framework: Jan 21 23:55:43.586: eap_fast_auth.c-AUTH-EVENT: TLS_DHE_RSA_WITH_AES_128_CBC_SHA proposed...  
*EAP Framework: Jan 21 23:55:43.586: eap_fast_auth.c-AUTH-EVENT: TLS_RSA_WITH_AES_128 proposed...  
*EAP Framework: Jan 21 23:55:43.586: eap_fast_auth.c-AUTH-EVENT: TLS_RSA_WITH_RC4_128 proposed...  
*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-EVENT: Proposed ciphersuite(s):  
*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-EVENT: Unknown ciphersuite 255  
*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-EVENT: Unknown ciphersuite 49188  
  
*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-EVENT: Unknown ciphersuite 103  
*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-EVENT: Unknown ciphersuite 57  
*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-EVENT: TLS_DHE_RSA_WITH_AES_128_CBC_SHA  
*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-EVENT: Unknown ciphersuite 22  
*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-EVENT: Unknown ciphersuite 61  
  
*EAP Framework: Jan 21 23:55:43.587: eap_fast.c-EVENT: TLS_RSA_WITH_AES_128_CBC_SHA  
*EAP Framework: Jan 21 23:55:43.587: eap_fast.c-EVENT: Unknown ciphersuite 10  
*EAP Framework: Jan 21 23:55:43.587: eap_fast.c-EVENT: Unknown ciphersuite 49159  
*EAP Framework: Jan 21 23:55:43.587: eap_fast.c-EVENT: Unknown ciphersuite 49169  
*EAP Framework: Jan 21 23:55:43.587: eap_fast.c-EVENT: TLS_RSA_WITH_RC4_128_SHA  
*EAP Framework: Jan 21 23:55:43.587: eap_fast.c-EVENT: Unknown ciphersuite 4  
*EAP Framework: Jan 21 23:55:43.592: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet(): EAP Fast NoData (0x2b)  
*EAP Framework: Jan 21 23:55:43.592: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b  
*EAP Framework: Jan 21 23:55:43.592: eap_fast_auth.c-AUTH-EVENT: Process Response (EAP handle = c4000000)  
*EAP Framework: Jan 21 23:55:43.592: eap_fast_auth.c-AUTH-EVENT: Received ACK from peer  
*EAP Framework: Jan 21 23:55:43.592: eap_fast.c-EVENT: Free context (EAP handle = c4000000)
```

An engineer deployed a Cisco WLC using local EAP. Users who are configured for EAP- PEAP cannot connect to the network. Based on the local EAP debug controller provided, why is the client unable to connect?

- A. The client is falling to accept certificate.
- B. The Cisco WLC is configured for the incorrect date.
- C. The user is using invalid credentials.
- D. The Cisco WLC local EAP profile is misconfigured

Correct Answer: A

QUESTION 3

An engineer wants to upgrade the APs in a Cisco FlexConnect group. To accomplish this upgrade, the FlexConnect AP



Upgrade setting will be used One AP of each model with the lowest MAC address in the group must receive the upgrade directly from the controller.

Which action accomplishes this direct upgrade?

- A. Reboot all APs before the upgrade.
- B. Remove the APs from the group
- C. Do not set any master APs. 9 0
- D. Allocate the master APs to different groups

Correct Answer: D

QUESTION 4

DRAG DROP

A wireless engineer wants to schedule monthly security reports in Cisco Prime infrastructure. Drag and drop the report the from the left onto the expected results when the report is generated on the right.

Select and Place:

Adaptive wIPS Alarm Summary	Displays a summarized count of all rogue access points on your network
Adhoc Rogue Count Summary	Displays a summary of security alarm trends over a period of time
Rogue AP Count Summary	Displays a summarized count of all ad hoc rogue access points
Security Alarm Trending Summary	Displays a summary of all adaptive wIPS alarms on your network

Correct Answer:



	Rogue AP Count Summary
	Security Alarm Trending Summary
	Adhoc Rogue Count Summary
	Adaptive wIPS Alarm Summary

QUESTION 5

Refer to the exhibit.

RADIUS Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret

Enable KeyWrap ⓘ

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

CoA Port

The security team has implemented ISE as a AAA solution for the wireless network. The wireless engineer notices that though clients can authenticate successfully, the ISE policies that are designed to place them on different interfaces are not working. Which configuration must be applied in the RADIUS Authentication Settings section from the ISE Network Device page?

- A. Disable KeyWrap
- B. Change the CoA Port
- C. Correct the shared secret.
- D. Use ASCII for the key input format

Correct Answer: B



QUESTION 6

An engineer must implement intrusion protection the WLAN. The AP coverage is adequate and on- channel attacks are the primary concern. The building is historic, which makes adding APs difficult. Which Ap mode and submode must be implemented?

- A. Ap mode: local, Ap submode: WIPS
- B. Ap mode: monitor, Ap submode: WIPS
- C. Ap mode: monitor, Ap submode: none
- D. Ap mode: local, Ap submode: none

Correct Answer: A

the on-channel says no need to scan other channels.

QUESTION 7

An engineer wants the wireless voice traffic class of service to be used to determine the queue order for packets received, and then have the differentiated services code point set to match when it is resent to another port on the switch. Which configuration is required in the network?

- A. Platinum QoS configured on the WLAN
- B. WMM set to required on the WLAN
- C. msl qos trust dscp configured on the controller switch port
- D. msl qos trust cos configured on the controller switch port

Correct Answer: D

QUESTION 8

A wireless network has been implemented to enable multicast video to be streamed reliably over the wireless link to the wireless to the wireless users. After a client reports that the video is unable to stream the administrator determines that the client is connecting a data rate of 12 Mbps and is trying to stream to a void multicast address on the network. Which two actions must be applied? (Choose two.)

- A. Allow RTSP stream the video due to wireless multicast not using acknowledgments.
- B. Allow multicast direct to work correctly and multicast-direct to be enabled globally.
- C. Change the WLAN QoS value to Bronze for the WLANs on the controller.
- D. Turn off IGMP snooping for all the configured WLANS on the controller.
- E. Implement video stream for the multicast video on the controller



Correct Answer: BE

QUESTION 9

The marketing department creates a promotion video for the branch store. Only interested hosts must receive the video over wireless multicast. What allows this feature?

- A. DCA
- B. WMM
- C. WMF
- D. TPC

Correct Answer: C

QUESTION 10

Refer to the exhibit.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port
1	Permit	0.0.0.0 / 0.0.0.0	10.230.1.45 / 255.255.255.255	Any	Any	Any
2	Permit	10.230.1.45 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any
3	Permit	0.0.0.0 / 0.0.0.0	10.225.49.15 / 255.255.255.255	Any	Any	Any
4	Permit	10.225.49.15 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any
5	Permit	0.0.0.0 / 0.0.0.0	10.230.1.61 / 255.255.255.255	UDP	DHCP Client	DHCP Server
6	Permit	10.230.1.61 / 255.255.255.255	0.0.0.0 / 0.0.0.0	UDP	DHCP Server	DHCP Client
7	Permit	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any
8	Permit	173.194.0.0 / 255.255.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any
9	Permit	0.0.0.0 / 0.0.0.0	74.125.0.0 / 255.255.0.0	Any	Any	Any
10	Permit	74.125.0.0 / 255.255.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any
11	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any

An ACL is configured to restrict access for BYOD clients. The ACL must redirect devices to the guest portal. To which two devices on the local network must the ACL allow access other than the DHCP server? (Choose two.)

- A. SNMP server B. Cisco ISE
- C. DNS server
- D. WLCD



E. RADIUS server

Correct Answer: BC

QUESTION 11

Which three characteristics of a rogue AP pose a high security risk? (Choose three.)

- A. open authentication
- B. high RSSI
- C. foreign SSID
- D. accepts clients
- E. low RSSI
- F. distant location

Correct Answer: ACD

https://www.cisco.com/c/en/us/td/docs/wireless/controller/74/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_010111001.html

QUESTION 12

You plan to implement Cisco Identity Based Networking Services on a Cisco Catalyst 3850 Series Switch. Which switch command is required when configuring downloadable ACLs?

- A. authentication display new-style
- B. ip device tracking
- C. dot1x system-auth-control
- D. aaa session-id common

Correct Answer: B

QUESTION 13

An engineer added more APs to newly renovated areas in building. The engineer is now receiving Out-of-Sync alarms on Cisco Prime Infrastructure. Which two actions resolve this issue? (Choose two.)

- A. Manually synchronize from Cisco Prime Infrastructure.
- B. Manually synchronize from MSE.



- C. Enable automatic synchronization on Cisco Prime Infrastructure.
- D. Enable automatic synchronization on MSE.
- E. Add new APs to maps on Cisco Prime Infrastructure.

Correct Answer: BD

ref: https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-5/user/guide/bk_CiscoPrimeInfrastructure_3_5_0_UserGuide/bk_CiscoPrimeInfrastructure_3_5_0_UserGuide_chapter_0100110.html#con_1301578:~:text=NEs%20with%20MSE-,Set%20Up%20Synchronization%20Between%20MSE%20Databases%20and%20Product%20Database,-Manual%20synchronization%20of

QUESTION 14

DRAG DROP

A network engineer must get an autonomous AP to authenticate to the upstream switch via IEEE 802.1 X. Drag and drop the commands from the left onto the right to complete the configuration.

Select and Place:



```
ap(config-if)#dot1x credentials [PROFILE NAME]
```

```
ap(config-dot1x-creden)#password {0 | 7 | LINE}
```

```
ap(config)#dot1x credentials [PROFILE NAME]
```

```
ap(config-dot1x-creden)#username username
```

```
ap(config)#interface gigabitethernet 0
```

step 1

step 2

step 3

step 4

step 5

Correct Answer:



```
ap(config)#dot1x credentials [PROFILE NAME]
```

```
ap(config-dot1x-creden)#username username
```

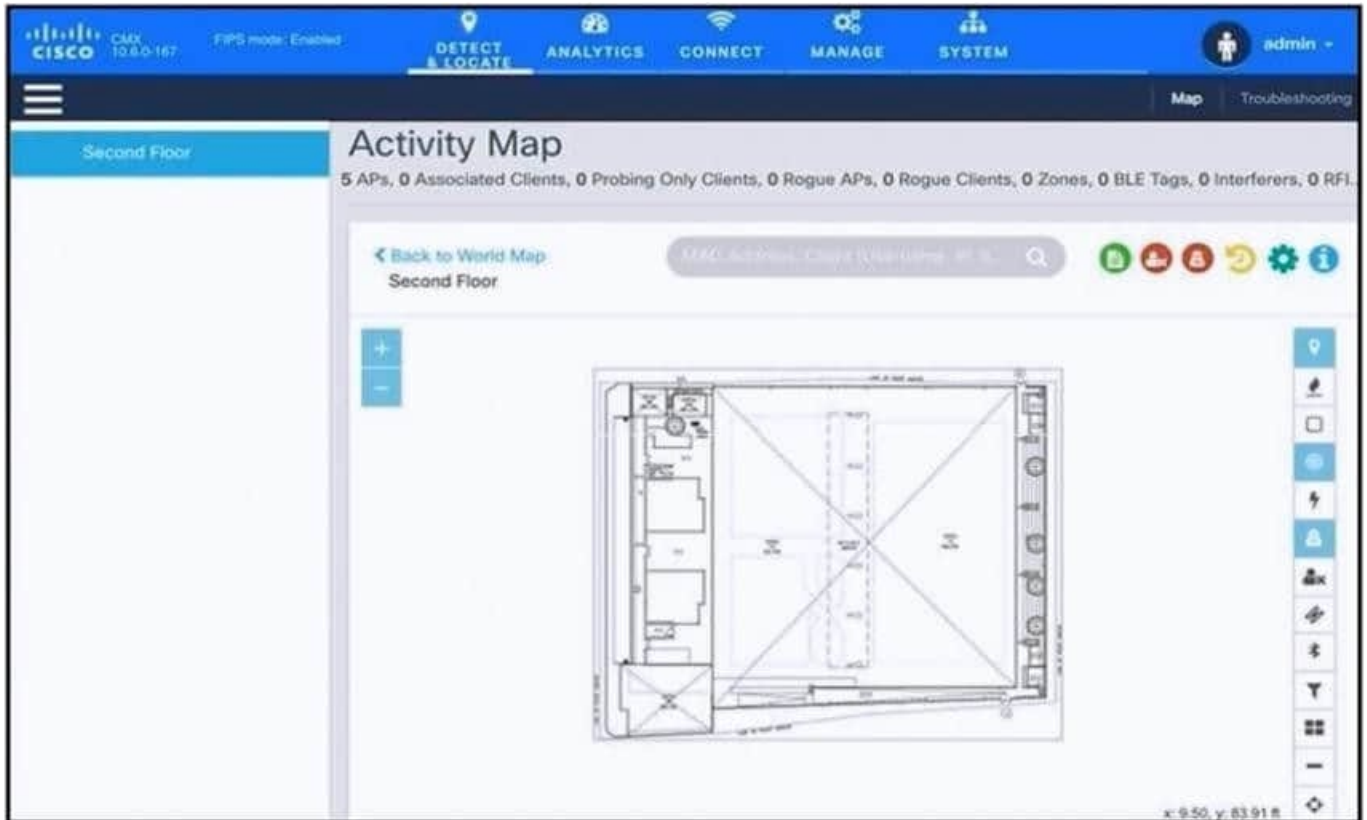
```
ap(config-dot1x-creden)#password {0 | 7 | LINE}
```

```
ap(config)#interface gigabitethernet 0
```

```
ap(config-if)#dot1x credentials [PROFILE NAME]
```

QUESTION 15

Refer to the exhibit.



An engineer has deployed the Cisco CMX solution to track and detect the number of users who visit the office each day. The CMX dashboard is not showing any data. Which action resolves this issue?

- A. Configure Single Sign-On authentication.
- B. Add the WLCs to CMX.
- C. Copy the exported Maps from CMX server to PI using SCP.
- D. Install an evaluation license to CMX server.

Correct Answer: B

https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-4/cmxcfg/b_cg_cmxc104/the_cisco_cmxc_detect_and_locate_service.html#:~:text=Wireless%20Controllers,-,Add%20controllers,-%E2%80%94For%20information%20about

[Latest 300-430 Dumps](#)

[300-430 PDF Dumps](#)

[300-430 Study Guide](#)