# Cisco

# 300-430

## Implementing Cisco Enterprise Wireless Networks (300-430 ENWLSI)

**Exams Boost**

Boost Up Your Career

## For More Information – Visit link below:

## https://www.examsboost.com/

## Product Version

# Latest Version: 16.2

## Question: 1

On a branch office deployment, it has been noted that if the FlexConnect AP is in standalone mode and loses connection to the WLC, all clients are disconnected, and the SSID is no longer advertised. Considering that FlexConnect local switching is enabled, which setting is causing this behavior?

A. ISE NAC is enabled
B. 802.11r Fast Transition is enabled
C. Client Exclusion is enabled
D. FlexConnect Local Auth is disabled

**Answer: D**

Explanation:
When FlexConnect APs are in standalone mode due to losing connection to the WLC, they should still be able to serve clients if local switching and authentication are enabled. The issue described occurs because FlexConnect Local Authentication is disabled. With local auth enabled, the AP can authenticate clients directly, without needing to communicate with the WLC, thus allowing the SSID to remain advertised and clients to stay connected even if the WLC is unreachable. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

## Question: 2

An engineer must implement intrusion protection on the WLAN. The AP coverage is adequate and onchannel 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: none
B. AP mode: monitor, AP submode: WIPS
C. AP mode: monitor, AP submode: none
D. AP mode: local, AP submode: WIPS

**Answer: B**

Explanation:
In a historic building where adding APs is challenging, the best approach to implement intrusion protection with a focus on on-channel attacks is to use APs in monitor mode with the Wireless Intrusion Prevention System (WIPS) submode. This setup allows the APs to dedicate their time to scanning the environment for threats without serving clients, which is suitable given the adequate coverage and the need to monitor for attacks. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and

## Question: 3

An engineer is implementing a FlexConnect group for access points at a remote location using local switching but central DHCP. Which client feature becomes available only if this configuration is changed?

A. multicast
B. static IP
C. fast roaming
D. mDNS

## Answer: C

Explanation:
In a FlexConnect group with local switching but central DHCP, clients can use features like multicast and static IP without any issues. However, fast roaming, which allows clients to move seamlessly between access points with minimal delay, requires the access points to handle client information locally. If the configuration is changed to allow local DHCP, then the access points can cache client credentials, enabling fast roaming.
Reference :=
CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide Cisco documentation on FlexConnect configurations

## Question: 4

A FlexConnect remote office deployment is using five 2702i APs indoors and two 1532i APs outdoors. When a code upgrade is performed and FlexConnect Smart AP Image Upgrade is leveraged, but no FlexConnect Master AP has been configured, how many image transfers between the WLC and APs will occur?

A. 1
B. 2
C. 5
D. 7

## Answer: B

Explanation:
When using FlexConnect Smart AP Image Upgrade without a configured FlexConnect Master AP, the WLC will transfer the image to one indoor AP and one outdoor AP separately. Each AP model needs a different firmware image due to hardware differences. Therefore, there will be two image transfers from the WLC:

one for the 2702i APs and another for the 1532i APs.
Reference :=
CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide
Cisco documentation on FlexConnect Smart AP Image Upgrade

## Question: 5

Where is a Cisco OEAP enabled on a Cisco Catalyst 9800 Series Wireless Controller?

A. RF Profile
B. Flex Profile
C. Policy Profile
D. AP Join Profile

## Answer: B

Explanation:
The Cisco OfficeExtend Access Point (OEAP) feature is enabled on a Cisco Catalyst 9800 Series Wireless Controller through the Flex Profile. The Flex Profile allows for the configuration of various settings specific to FlexConnect deployments, including OEAP settings, which enable remote workers to connect to the corporate network securely.
Reference :=
CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide
Cisco documentation on Catalyst 9800 Series Wireless Controllers

# Thank You for Trying Our Product

For More Information – **Visit link below:**

## https://www.examsboost.com/

**15 USD Discount Coupon Code:**

## G74JA8UF

# FEATURES

- ✓ **90 Days Free Updates**
- ✓ **Money Back Pass Guarantee**
- ✓ **Instant Download or Email Attachment**
- ✓ **24/7 Live Chat Support**
- ✓ **PDF file could be used at any Platform**
- ✓ **50,000 Happy Customer**