Recommendations and Limitations

Recommendations

This section provides some recommendations that you can keep in mind while using the Cisco Catalyst 9800 Series Wireless Controller configuration model.

- When you design your Cisco Catalyst wireless network, it is important to consider site tags and the way these are mapped to APs. For the best performance of your Cisco Catalyst 9800 Series Wireless Controller, it is recommended that you:
  - Use custom site tags and not the default site tag.
  - Assign the same site tag to all the APs in the same roaming domain.
  - Limit the number of APs to 500 per site tag whenever possible.
  - Do not exceed the following maximum number of APs per site tag:

Table 1: Maximum Number of APs per Site Tag

Platform	Maximum Number of APs per Site Tag
• Cisco Catalyst 9800-80 Series Wireless Controller (medium and large) • Cisco Catalyst 9800-CL Wireless Controller for Cloud (medium and large)	1600
Cisco Catalyst 9800-40 Series Wireless Controller	800
Any other Cisco Catalyst 9800 platform	Equal to the maximum number of APs supported.

- When designing your policy tag assignment, ensure that all APs in the same roaming domain should have the same policy profile. In case you need to assign different policies, then we recommend that you use Cisco IOS XE Amsterdam 17.3.x and later releases.
- We recommend that you limit the number of SSIDs configured on the controller. You can configure 16 simultaneous WLANs or SSIDs (per radio on each AP). Because each WLAN or SSID needs separate probe responses and beacons transmitted at the lowest mandatory rate, the RF pollution increases as more SSIDs are added.

  Also, some smaller wireless stations such as PDAs, Wi-Fi phones, and barcode scanners cannot cope with a high number of Basic SSIDs (BSSIDs) over the air. This results in lockups, reloads, or association failures. It is recommended that you have one to three SSIDs for an enterprise, and one SSID for high-density designs. By using the AAA override feature, you can reduce the number of WLANs or SSIDs while assigning individual per-user VLAN/settings in a single-SSID scenario.
- Because you can modify the existing tags, create new ones, and attach these tags to APs in different ways, we recommend that you validate the tag configuration using the following command:

  ```
  Device# wireless config validate
  ```
- Do not mix clients with DHCP and static IP address on the same SSID when associating with a VLAN group.
- To enhance security, ensure that all clients obtain their IP addresses from the DHCP server. The DHCP-Required option in the Policy profile settings forces clients to request or renew a DHCP address every time they associate with a WLAN, before they are allowed to send or receive other traffic in the network. The DHCP-Required option allows for strict control over the IP addresses in use.
- Set the per-WLAN user idle timeout to 3600 seconds (60 minutes) to reduce the likelihood of client getting deleted when moving out of coverage areas or when the client is battery-operated and may go to sleep frequently.
- If you have devices that are still using Cisco Centralized Key Management, ensure that you change Cisco Centralized Key Management validation to 5 seconds to avoid roaming issues when using Cisco-based clients.

Restrictions for WLANs

- Do not configure pre-shared key (PSK) and Cisco Centralized Key Management in a WLAN, because this configuration is not supported.
- Ensure that the Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES) ciphers are enabled with Wi-Fi Protected Access (WPA1) configuration, else In-Service Software Upgrade (ISSU) may break during the upgrade process.
- When you change the WLAN profile name, the FlexConnect APs (using AP-specific VLAN mapping) will become WLAN-specific. If FlexConnect groups are configured, the VLAN mapping will become group-specific.
- Do not enable IEEE 802.1X Fast Transition on Flex local-authentication enabled WLAN, because the client association is not supported with Fast Transition 802.1X key management.
- Peer-to-peer blocking does not apply to multicast traffic.

- In FlexConnect, peer-to-peer blocking configuration cannot be applied only to a particular FlexConnect AP or a subset of APs. It is applied to all the FlexConnect APs that broadcast the SSID.
- The WLAN name and SSID can have up to 32 characters.
- WLAN and SSID names support only the following ASCII characters:
  - Numerals: 48 through 57 hex (0 to 9)
  - Alphabets (uppercase): 65 through 90 hex (A to Z)
  - Alphabets (lowercase): 97 through 122 hex (a to z)
  - ASCII space: 20 hex
  - Printable special characters: 21 through 2F, 3A through 40, and 5B through 60 hex, that is: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
- WLAN name cannot be a keyword; for example, if you try to create a WLAN with the name as 's' by entering the **wlan s** command, it results in the shutting down of all WLANs because 's' is used as a keyword for shutdown.
- You cannot map a WLAN to VLAN 0. Similarly, you cannot map a WLAN to VLANs 1002 to 1006.
- Dual stack clients with a static-IPv4 address are not supported.
- In a dual-stack (with IPv4 and IPv6 configured) Cisco Catalyst 9800 Series Wireless Controller, if an AP tries to join the controller with the IPv6 tunnel before the IPv4 tunnel gets cleared, you will see a traceback, and the AP join will fail.
- When creating a WLAN with the same SSID, you must create a unique profile name for each WLAN.
- When multiple WLANs with the same SSID is assigned to the same AP radio, you must have a unique Layer 2 security policy so that clients can safely select between these WLANs.
- The SSID that is sent as part of the user profile works only if the **aaa override** command is configured.
- RADIUS server overwrite is not configured on a per WLAN basis, but rather on a per AAA server-group basis.
- Downloadable ACL (DACL) is not supported in FlexConnect mode or local mode.
- You cannot mix open configuration models with CLI-based, GUI-based, or DNA Center-based configurations. However, if you decide to use multiple model types, these must remain independent of each other. For example, in open configuration models, you can only manage configurations that have been created using an open configuration model, not a CLI-based or GUI-based model. Configurations that are created using open configuration models cannot be modified using a GUI-based model, or CLI-based model, or any other model.

Caution Some clients might not be able to connect to WLANs properly if they detect the same SSID with multiple security policies. Use this WLAN feature with care.

Restrictions for Peer-to-Peer Blocking

- Peer-to-peer blocking does not apply to multicast traffic.
- Peer-to-peer blocking is not enabled by default.
- In FlexConnect, peer-to-peer blocking configuration cannot be applied only to a particular FlexConnect AP or a subset of APs. It is applied to all the FlexConnect APs that broadcast the SSID.
- Unified solution for central switching clients supports peer-to-peer upstream-forward. However, this is not supported in the FlexConnect solution; it is treated as peer-to-peer drop, and client packets are dropped.

Restrictions for DHCP for WLANs

- If you override the DHCP server in a WLAN, you must ensure that you configure the underlying Cisco IOS configuration in such a way that the DHCP server is reachable.
- WLAN DHCP override works only if DHCP service is enabled on the device.

  You can configure DHCP service in either of the following ways:

  - Configuring the DHCP pool on the device.
  - Configuring a DHCP relay agent on the SVI. Note that the VLAN of the SVI must be mapped to the WLAN where DHCP override is configured.

Topic 2.1

Restrictions for FlexConnect DHCP-Required

The following are the restrictions and limitations for the FlexConnect DHCP-Required feature:

- The DHCP-Required feature is applicable for IPv4 addresses only.
- The IP-MAC binding can be pushed to other APs only through the custom policy profile. IP-MAC binding is not available in the default policy. The mapping is propagated to all the APs in the same custom policy profile.
- The DHCP-Required feature works on IP-MAC binding basis and is not supported with the third-party work group bridge (WGB), where WGB wired client information is not shared to AP by the WGB.