# Infrastructure



# Application Visibility and Control

- Description— Application Visibility should be enabled. Clicking **Fix it Now** enables Application Visibility on all WLANs.
- Status:
  - Selected—Enabled on all WLANs
  - Unselected—Disabled on all WLANs
- CLI Option—Enable AVC on a WLAN by entering this command:

```
(Cisco Controller) >config wlan avc wlan-id visibility enable
```

# Load Balancing

- Description—Load balancing should be enabled. For time sensitive application such as voice, it can cause roaming issues. Therefore, it is recommended to test before enabling load balancing on the WLANs. Clicking **Fix it Now** enables load balancing on all WLANs, which may impact service at the time.
- Status:
  - Selected—Enabled on all WLANs
  - Unselected—Disabled on all WLANs
- CLI Option—Enable load balancing on a WLAN by entering this command:

```
(Cisco Controller) >config wlan load-balance allow enable wlan-id
```

# Local Profiling

- Description—Local profiling should be enabled. Clicking **Fix it Now** enables local profiling (DHCP/HTTP) on all WLANs; this may impact service at the time.
- Status:
  - Selected—Enabled on all WLANs. It is shown in Green state if RADIUS profiling is enabled
  - Unselected—Disabled
- CLI Option—Enable local profiling (DHCP/HTTP) on all WLANs by entering this command:

```
(Cisco Controller) >config wlan profiling local all enable
```

# NTP

- Description— NTP server should be used to sync the WLC time.

  Network Time Protocol (NTP) is very important for several features. It is mandatory to use NTP synchronization on WLCs if you use any of these features: Location, SNMPv3, access point authentication, or MFP. The WLC supports synchronization with NTP using authentication.
- Status
  - Selected—Configured
  - Unselected—Not configured
- CLI Option:
  - Enable NTP server by entering this command:

    ```
    (Cisco Controller) >config time ntp server ntp-server-index ntp-server-ip-address
    ```
  - Enable NTP authentication by entering this command:

```
(Cisco Controller) >config time ntp auth enable ntp-server-index
(Cisco Controller) >config time ntp key-auth add key-index
```

# Fast SSID

- Description—Fast SSID should be enabled. Clicking **Fix it Now** enables fast SSID.
- Status:
  - Selected—Enabled
  - Unselected—Disabled
- CLI Option—Enable fast SSID by entering this command:

```
(Cisco Controller) >config network fast-ssid-change
```

# mDNS Snooping

- Description—mDNS snooping should be enabled. Clicking **Fix it Now** enables mDNS snooping.
- Status:
  - Selected—Enabled
  - Unselected—Disabled
- CLI Option—Enable mDNS snooping by entering this command:

```
(Cisco Controller) >config mdns snooping enable
```

# Management over Wireless

- Description—The Cisco WLAN solution Management over Wireless feature allows Cisco WLAN solution operators to monitor and configure local WLCs using a wireless client. Management over wireless should be disabled for security reasons. Clicking **Fix it Now** disables management over wireless.
- Status:
  - Selected—Enabled
  - Unselected—Disabled
- CLI Option—Disable management over wireless by entering this command:

```
(Cisco Controller) >config network mgmt-via-wireless disable
```

# Secure Web Access

- Description—Secure Web Access should be enabled. Web Access should be disabled. Clicking **Fix it Now** enables HTTPS and disables HTTP.
- Status:
  - Selected—HTTPS enabled; HTTP disabled
  - Unselected—HTTPS enabled, HTTP enabled or HTTPS disabled, HTTP enabled
- CLI to configure
  - Disable the web mode to deny users to access the WLC GUI using http://ip-address, by entering this command:

    ```
    (Cisco Controller) >config network webmode disable
    ```

  - Enable Secure Web Access mode to allow users to access the WLC GUI using https://ip-address, by entering this command:

    ```
    (Cisco Controller) >config network secureweb enable
    ```

# Aironet IE

- Description—CCX Aironet IE feature should be disabled. Clicking **Fix it Now** disables CCX Aironet IE.

  Aironet IE is a Cisco proprietary attribute used by Cisco devices for better connectivity. It contains information, such as the access point name, load, number of associated clients, and so on sent out by the access point (AP) in the beacon and probe responses of the WLAN. The Cisco Client Extensions (CCX) clients use this information to choose the best AP with which to associate.

  The CCX software is licensed to manufacturers and vendors of third-party client devices. The CCX code resident on these clients enables them to communicate wirelessly with Cisco APs and to support Cisco features that other client devices do not. The features are related to increased security, enhanced performance, fast roaming, and power management.

  Aironet IE is optional for CCX based clients, however it can cause compatibility issues with some types of wireless clients. The recommendation is to enable for WGB and Cisco voice, but for general production network, it can be beneficial to disable Aironet IE after testing.
- Status:
  - Selected—CCX Aironet IE disabled on all WLANs.
  - Unselected—CCX Aironet IE enabled on all WLANs.
- CLI Option—Disable support for Aironet IEs for a particular WLAN by entering this command:

  ```
  (Cisco Controller) >config wlan ccx aironetIeSupport disable wlan-id
  ```

# Multicast Forwarding

- Description—Use multicast forwarding mode for the best performance with less bandwidth utilization.

  Use multicast forwarding mode for the best performance with less bandwidth utilization. Networks with large IPv6 client counts, heavy multicast application such as Video Streaming, or mDNS without mDNS proxy, would benefit greatly with multicast mode.

- Status:
  - Selected—Enabled
  - Unselected—Disabled
- To verify the multicast mode on the controller:

```
(Cisco Controller) >show network summary
```

- To configure multicast-multicast operations:

```
(Cisco Controller) >config network multicast mode multicast multicast-group-ip-address
(Cisco Controller) >config network multicast global enable
```

**Note**

- The multicast address is used by the WLC to forward traffic to Access Points (APs). It is important that the multicast address does not match another address in use on your network by other protocols. For example, if you use 224.0.0.251, it breaks mDNS used by some third party applications. We recommend that the address be in the private range (239.0.0.0 – 239.255.255.255, which does not include 239.0.0.x and 239.128.0.x). It is also important that the multicast IP address be set to a different value on each WLC. You would not want a WLC that speaks to its APs to reach the APs of another WLC.
- If the APs are on a different subnetwork than the one used on the management interface, your network infrastructure must provide multicast routing between the management interface subnet and the AP subnetwork.

# Multicast Mobility

- Description—Allows WLCs to announce messages to all mobility peers instead of individual WLC with CPU and network benefits. Ensure multicast traffic is passing between WLCs when their management is on different subnets.
- Status:
  - Selected—Enabled
  - Unselected—Disabled
- CLI Option—Configure the mobility multicast mode by entering this command:

```
(Cisco Controller) >config mobility multicast-mode enable local-multicast-address
```

# Controller High Availability

- Description—High Availability should be enabled. If redundancy mode is not set, assume HA is not enabled.
- Status:
  - Selected—Enabled
  - Unselected—Disabled