Cisco CleanAir

Configuring Cisco CleanAir on the Controller

Configuring Cisco CleanAir on the Cisco Wireless LAN Controller (GUI)

Step 1 Choose **Wireless** > **802.11a/n/ac or 802.11b/g/n > CleanAir** to open the **802.11a (or 802.11b) > CleanAir** page.

Step 2 Select the **CleanAir** check box to enable Cisco CleanAir functionality on the 802.11a/n or 802.11b/g/n network, or unselect it to prevent the Cisco WLC from detecting spectrum interference. By default, the value is not selected.

Step 3 Select the **Report Interferers** check box to enable the Cisco CleanAir system to report any detected sources of interference, or unselect it to prevent the Cisco WLC from reporting interferers. The default value is selected.

Note Device Security alarms, Event Driven RRM, and the Persistence Device Avoidance algorithm do not work if Report Interferers are disabled.

Step 4 Select the **Persistent Device Propagation** check box to enable propagation of information about persistent devices that can be detected by CleanAir. Persistent device propagation enables you to propagate information about persistent devices to the neighboring access points connected to the same Cisco WLC. Persistent interferers are present at the location and interfere with the WLAN operations even if they are not detectable at all times.

Step 5 Ensure that any sources of interference that need to be detected and reported by the Cisco CleanAir system appear in the Interferences to Detect box and any that do not need to be detected appear in the Interferences to Ignore box. Use the > and < buttons to move interference sources between these two boxes. By default, all interference sources are detected. The possible sources of interference that you can choose are as follows:

- **Bluetooth Paging Inquiry—**A Bluetooth discovery (802.11b/g/n only)
- **Bluetooth Sco Acl—**A Bluetooth link (802.11b/g/n only)
- **Generic DECT—**A digital enhanced cordless communication (DECT)-compatible phone
- **Generic TDD—**A time division duplex (TDD) transmitter
- **Generic Waveform—**A continuous transmitter

- **Jammer—**A jamming device
- **Microwave—**A microwave oven (802.11b/g/n only)
- **Canopy—**A canopy bridge device
- **Spectrum 802.11 FH—**An 802.11 frequency-hopping device (802.11b/g/n only)
- **Spectrum 802.11 inverted—**A device using spectrally inverted Wi-Fi signals
- **Spectrum 802.11 non std channel—**A device using nonstandard Wi-Fi channels
- **Spectrum 802.11 SuperG—**An 802.11 SuperAG device
- **Spectrum 802.15.4—**An 802.15.4 device (802.11b/g/n only)
- **Video Camera—**An analog video camera
- **WiMAX Fixed—**A WiMAX fixed device (802.11a/n/ac only)
- **WiMAX Mobile—**A WiMAX mobile device (802.11a/n/ac only)
- **XBox—**A Microsoft Xbox (802.11b/g/n only)

Note Access points that are associated to the Cisco WLC send interference reports only for the interferers that appear in the Interferences to Detect box. This functionality allows you to filter out interferers that you do not want as well as any that may be flooding the network and causing performance problems for the Cisco WLC or Prime Infrastructure. Filtering allows the system to resume normal performance levels.

Step 6 Configure Cisco CleanAir alarms as follows:

a) Select the **Enable AQI (Air Quality Index) Trap** check box to enable the triggering of air quality alarms, or unselect the box to disable this feature. The default value is selected.

b) If you selected the **Enable AQI Trap** check box in *Step a*, enter a value between 1 and 100 (inclusive) in the AQI Alarm Threshold text box to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 35.

c) Enter the **AQI Alarm Threshold (1 to 100)** that you want to set. An alarm is generated when the air quality reaches a threshold value. The default is 35. Valid range is from 1 and 100.

d) Select the **Enable trap for Unclassified Interferences** check box to enable the AQI alarm to be generated upon detection of unclassified interference beyond the severity threshond specified in the **AQI Alarm Threshold**. Unclassified interferences are interferences that are detected but do not correspond to any of the identifiable interference types.

e) Enter the **Threshold for Unclassified category trap (1 to 99)**. Enter a value from 1 and 99. The default is 20. This is the severity index threshold for an unclassified interference category.

f) Select the **Enable Interference Type Trap** check box to trigger interferer alarms when the Cisco WLC detects specified device types, or unselect it to disable this feature. The default value is selected

g) Make sure that any sources of interference that need to trigger interferer alarms appear in the Trap on These Types box and any that do not need to trigger interferer alarms appear in the Do Not Trap on These Types box. Use the > and < buttons to move interference sources between these two boxes. By default, all interference sources trigger interferer alarms.
For example, if you want the Cisco WLC to send an alarm when it detects a jamming device, select the **Enable Interference Type Trap check box** and move the jamming device to the Trap on These Types box.

Step 7 Click **Apply**.

Step 8 Trigger spectrum event-driven radio resource management (RRM) to run when a Cisco CleanAir-enabled access point detects a significant level of interference as follows:

a) Look at the **EDRRM** field to see the current status of spectrum event-driven RRM and, if enabled, the Sensitivity Threshold field to see the threshold level at which event-driven RRM is invoked.

b) If you want to change the current status of event-driven RRM or the sensitivity level, click **Change Settings**. The **802.11a (or 802.11b) > RRM > Dynamic Channel Assignment (DCA)** page appears.

c) Select the **EDRRM** check box to trigger RRM to run when an access point detects a certain level of interference, or unselect it to disable this feature. The default value is selected.

d) If you selected the **EDRRM** check box in *Step c*, choose **Low**, **Medium**, **High,** or **Custom** from the **Sensitivity Threshold** drop-down list to specify the threshold at which you want RRM to be triggered. When the interference for the access point rises above the threshold level, RRM initiates a local dynamic channel assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity
If you selected the EDRRM sensitivity threshold as custom, you must set a threshold value in the Custom Sensitivity Threshold field. The default sensitivity is 35.

The EDRRM AQ threshold value for low sensitivity is 35, medium sensitivity is 50, and high sensitivity is 60.

e) To configure rogue duty cycle, select the **Rogue Contribution** check box and then specify the **Rogue Duty-Cycle** in percentage value. The default value of **Rogue Duty-Cycle** is 80%.

f) Click **Apply**.

Step 9 Click **Save Configuration**.

Configuring Cisco CleanAir on the Cisco Wireless LAN Controller (CLI)

Step 1 Configure Cisco CleanAir functionality on the 802.11 network by entering this command:
config {**802.11a** | **802.11b**} **cleanair** {**enable** | **disable**} *all*

If you disable this feature, the Cisco WLC does not receive any spectrum data. The default value is enable.

Step 2 Enable CleanAir on all associated access points in a network:
config {**802.11a** | **802.11b**} **cleanair enable network**

You can enable CleanAir on a 5-GHz radio of mesh access points.

Step 3 Configure interference detection and specify sources of interference that need to be detected by the Cisco CleanAir system by entering this command:
config {**802.11a** | **802.11b**} **cleanair device** {**enable** | **disable**} *type*

where you choose the *type* as one of the following:

- **802.11-fh—**An 802.11 frequency-hopping device (802.11b/g/n only)
- **802.11-inv—**A device using spectrally inverted Wi-Fi signals
- **802.11-nonstd—**A device using nonstandard Wi-Fi channels

- **802.15.4—**An 802.15.4 device (802.11b/g/n only)
- **all—**All interference device types (this is the default value)
- **bt-discovery—**A bluetooth discovery (802.11b/g/n only)
- **bt-link—**A bluetooth link (802.11b/g/n only)
- **canopy—**A canopy device
- **cont-tx—**A continuous transmitter
- **dect-like—**A digital enhanced cordless communication (DECT)-compatible phone
- **jammer—**A jamming device
- **mw-oven—**A microwave oven (802.11b/g/n only)
- **superag—**An 802.11 SuperAG device
- **tdd-tx—**A time division duplex (TDD) transmitter
- **video camera—**An analog video camera
- **wimax-fixed—**A WiMAX fixed device
- **wimax-mobile—**A WiMAX mobile device
- **xbox—**A Microsoft Xbox (802.11b/g/n only)

Note Access points that are associated to the Cisco WLC send interference reports only for the interference types specified in this command. This functionality allows you to filter out interferers that may be flooding the network and causing performance problems for the Cisco WLC or Prime Infrastructure. Filtering allows the system to resume normal performance levels.

Step 4 Configure the triggering of air quality alarms by entering this command:
config {**802.11a** | **802.11b**} **cleanair alarm air-quality** {**enable** | **disable**}

The default value is enabled.

Step 5 Specify the threshold at which you want the air quality alarm to be triggered by entering this command:
config {**802.11a** | **802.11b**} **cleanair alarm air-quality threshold** *threshold*

where *threshold* is a value between 1 and 100 (inclusive). When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 35.

Step 6 Enable the triggering of interferer alarms by entering this command:
config {**802.11a** | **802.11b**} **cleanair alarm device** {**enable** | **disable**}
The default value is enable.

Step 7 Specify sources of interference that trigger alarms by entering this command:
config {**802.11a** | **802.11b**} **cleanair alarm device** *type* {**enable** | **disable**} where you choose the *type* as one of the following:

- **802.11-fh—**An 802.11 frequency-hopping device (802.11b/g/n only)
- **802.11-inv—**A device using spectrally inverted Wi-Fi signals
- **802.11-nonstd—**A device using nonstandard Wi-Fi channels
- **802.15.4—**An 802.15.4 device (802.11b/g/n only)

- **all—**All interference device types (this is the default value)
- **bt-discovery—**A Bluetooth discovery (802.11b/g/n only)
- **bt-link—**A Bluetooth link (802.11b/g/n only)
- **canopy—**A canopy device
- **cont-tx—**A continuous transmitter
- **dect-like—**A digital enhanced cordless communication (DECT)-compatible phone
- **jammer—**A jamming device
- **mw-oven—**A microwave oven (802.11b/g/n only)
- **superag—**An 802.11 SuperAG device
- **tdd-tx—**A time division duplex (TDD) transmitter
- **video camera—**An analog video camera
- wimax-fixed**—**A WiMAX fixed device
- **wimax-mobile—**A WiMAX mobile device
- **xbox—**A Microsoft Xbox (802.11b/g/n only)

Step 8 Configure the triggering of air quality alarms for unclassified devices by entering this command:
config {**802.11a** | **802.11b**} **cleanair alarm unclassified** {**enable** | **disable**}

Step 9 Specify the threshold at which you want the air quality alarm to be triggered for unclassified devices by entering this command:
config {**802.11a** | **802.11b**} **cleanair alarm unclassified threshold** *threshold*

where *threshold* is a value from 1 and 99 (inclusive). When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 35.

Step 10 Trigger spectrum event-driven radio resource management (RRM) to run when a Cisco CleanAir-enabled access point detects a significant level of interference by entering these commands:
config advanced {**802.11a** | **802.11b**} **channel cleanair-event** {**enable** | **disable**}—Enables or disables spectrum event-driven RRM. The default value is disabled.

config advanced {**802.11a** | **802.11b**} **channel cleanair-event sensitivity** {**low** | **medium** | **high** | **custom**}—Specifies the threshold at which you want RRM to be triggered. When the interference level for the access point rises above the threshold level, RRM initiates a local dynamic channel assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while high represents an increased sensitivity. You can also set the sensitivity to a custom level of your choice. The default value is medium.

config advanced {**802.11a** | **802.11b**} **channel cleanair-event sensitivity threshold** *thresholdvalue***—**If you set the threshold sensitivity as custom, you must set a custom threshold value. The default is 35.

Step 11 Configure and monitor Interference Awareness by entering the following commands:

- **config advanced** {**802.11a** | **802.11b**} **channel cleanair-event** {**enable** | **disable**}
- **config advanced** {**802.11a** | **802.11b**} **channel cleanair-event rogue-contribution** {**enable** | **disable**}

- **config advanced** {**802.11a** | **802.11b**} **channel cleanair-event rogue-contribution duty-cycle** *value*
- **show** {**802.11a** | **802.11b**} **cleanair config**
- **debug airewave-director profile enable**
- **debug airewave-director channel enable**

Step 12 Enable persistent devices propagation by entering this command:
config advanced {**802.11a** | **802.11b**} **channel pda-prop** {**enable** | **disable**}

Step 13 Save your changes by entering this command:
save config

Step 14 See the Cisco CleanAir configuration for the 802.11a/n or 802.11b/g/n network by entering this command:
show {**802.11a** | **802.11b**} **cleanair config**

Information similar to the following appears:

```
(Cisco Controller) >show 802.11a cleanair config

Clean Air Solution............................... Disabled
Air Quality Settings:
    Air Quality Reporting........................ Enabled
    Air Quality Reporting Period (min)........... 15
    Air Quality Alarms........................... Enabled
      Air Quality Alarm Threshold................ 35
      Unclassified Interference.................. Disabled
      Unclassified Severity Threshold............ 20
Interference Device Settings:
    Interference Device Reporting................ Enabled
    Interference Device Types:
        TDD Transmitter.......................... Enabled
        Jammer................................... Enabled
        Continuous Transmitter................... Enabled
        DECT-like Phone.......................... Enabled
        Video Camera............................. Enabled
        WiFi Inverted............................ Enabled
        WiFi Invalid Channel..................... Enabled
        SuperAG.................................. Enabled
        Canopy................................... Enabled
        WiMax Mobile............................. Enabled
  WiMax Fixed.............................. Enabled
Interference Device Alarms................... Enabled
    Interference Device Types Triggering Alarms:
        TDD Transmitter.......................... Disabled
        Jammer................................... Enabled
        Continuous Transmitter................... Disabled
        DECT-like Phone.......................... Disabled
        Video Camera............................. Disabled
        WiFi Inverted............................ Enabled
        WiFi Invalid Channel..................... Enabled
        SuperAG.................................. Disabled
        Canopy................................... Disabled
        WiMax Mobile............................. Disabled
        WiMax Fixed.............................. Disabled
Additional Clean Air Settings:
    CleanAir ED-RRM State........................ Disabled
    CleanAir ED-RRM Sensitivity.................. Medium
    CleanAir ED-RRM Custom Threshold............. 50
    CleanAir Persistent Devices state............ Disabled
    CleanAir Persistent Device Propagation....... Enabled
```

Step 15 See the spectrum event-driven RRM configuration for the 802.11a/n/ac or 802.11b/g/n network by entering this command:
show advanced {**802.11a** | **802.11b**} *channel*

Information similar to the following appears:

```
Automatic Channel Assignment
  Channel Assignment Mode....................... AUTO
  Channel Update Interval....................... 600 seconds [startup]
  Anchor time (Hour of the day)................. 0
  Channel Update Contribution................... SNI
  CleanAir Event-driven RRM option............. Enabled
CleanAir Event-driven RRM sensitivity...... Medium
```

Configuring Cisco CleanAir on an Access Point

Configuring Cisco CleanAir on an Access Point (GUI)

Step 1 Choose **Wireless** > **Access Points > Radios > 802.11a/n/ac or 802.11b/g/n** to open the 802.11a/n/ac (or 802.11b/g/n) Radios page.

Step 2 Hover your cursor over the blue drop-down arrow for the desired access point and click **Configure**. The 802.11a/n/ac (or 802.11b/g/n) Cisco APs > Configure page appears.

The **CleanAir Capable** field shows whether this access point can support CleanAir functionality. If it can, go to the next step to enable or disable CleanAir for this access point. If the access point cannot support CleanAir functionality, you cannot enable CleanAir for this access point.

Note By default, the Cisco CleanAir functionality is enabled on the radios.

Step 3 Enable Cisco CleanAir functionality for this access point by choosing **Enable** from the CleanAir Status drop-down list. To disable CleanAir functionality for this access point, choose **Disable**. The default value is Enable. This setting overrides the global CleanAir configuration for this access point.

The **Number of Spectrum Expert Connections** text box shows the number of Spectrum Expert applications that are currently connected to the access point radio. Up to three active connections are possible.

Step 4 Click **Apply**.

Step 5 Click **Save Configuration**.

Step 6 Click **Back** to return to the 802.11a/n/ac (or 802.11b/g/n) Radios page.

Step 7 View the Cisco CleanAir status for each access point radio by looking at the **CleanAir Status** text box on the 802.11a/n/ac (or 802.11b/g/n) Radios page.

The Cisco CleanAir status is one of the following:

- **UP—**The spectrum sensor for the access point radio is currently operational (error code 0).
- **DOWN—**The spectrum sensor for the access point radio is currently not operational because an error has occurred. The most likely reason for the error is that the access point radio is disabled (error code 8). To correct this error, enable the radio.

- **ERROR—**The spectrum sensor for the access point radio has crashed (error code 128), making CleanAir monitoring nonoperational for this radio. If this error occurs, reboot the access point. If the error continues to appear, you might want to disable Cisco CleanAir functionality on the radio.
- **N/A—**This access point radio is not capable of supporting Cisco CleanAir functionality.

Note You can create a filter to make the 802.11a/n/ac Radios page or the 802.11b/g/n Radios page show only access point radios that have a specific Cisco CleanAir status (such as UP, DOWN, ERROR, or N/A). This feature is especially useful if your list of access point radios spans multiple pages, preventing you from viewing them all at once. To create a filter, click **Change Filter** to open the Search AP dialog box, select one or more of the CleanAir Status check boxes, and click **Find**. Only the access point radios that match your search criteria appear on the 802.11a/n/ac Radios page or the 802.11b/g/n Radios page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, CleanAir Status: UP).

Configuring Cisco CleanAir on an Access Point (CLI)

Step 1 Configure Cisco CleanAir functionality for a specific access point by entering this command:
config {**802.11a** | **802.11b**} **cleanair {enable | disable}***Cisco_AP*

Step 2 Save your changes by entering this command:
save config

Step 3 See the Cisco CleanAir configuration for a specific access point on the 802.11a/n/ac or 802.11b/g/n network by entering this command:
show ap config {802.11a | 802.11b} *Cisco_AP*

Information similar to the following appears:

```
Cisco AP Identifier.............................. 0
Cisco AP Name.................................... CISCO_AP3500
...
Spectrum Management Information
        Spectrum Management Capable.............. Yes
        Spectrum Management Admin State.......... Enabled
        Spectrum Management Operation State...... Up
        Rapid Update Mode........................ Disabled
        Spectrum Expert connection............... Disabled
   Spectrum Sensor State................. Configured (Error code = 0)
```

Note See step 7 of Configuring Cisco CleanAir on an Access Point (GUI), on page 7 for descriptions of the spectrum management operation states and the possible error codes for the spectrum sensor state.