Design Model Configuration

Introduction to Model Config Editor

Model Config allows you to define advanced customizations of the Cisco Validated Designs (CVDs) that are encapsulated within the provisioning applications. Model Configs are a set of model-based, discoverable, and customizable configuration capabilities, which you can deploy on your network devices with high-level service intent and device-specific CLI templates.

The Model Configs feature simplifies network provision by extracting complex device configurations and facilitating customizable network configurations using an intuitive GUI instead of device-specific CLIs. A common design is deployed to various device hardware platforms and software types in a uniform way. During deployments, the Cisco DNA Center infrastructure automatically validates and translates extracted designs to device-specific CLI commands.

To provision model config design, do the following:

1. Create a new model config design using the **Model Config Editor** window (menu icon > **Tools** > **Model Config Editor**).
2. Apply the model config design to different network profiles.
3. Using the provision workflow, apply the model config design that is specified in network profiles to a network device.

Supported Model Config Design Types

Cisco DNA Center supports the following wireless Model Config design types:

- AAA Radius attributes configuration
- Advanced SSID configuration
- CleanAir configuration
- Event driven RRM configuration
- Flex configuration
- Dot11ax configuration
- Global IPv6 configuration
- Multicast configuration
- RRM FRA configuration
- RRM general configuration

Discover and Create Designs from a Legacy Device

Instead of manually creating designs using the Model Config Editor, you can use the Discover Model Configs feature to discover the existing model configuration designs available on legacy devices and use them as a template to create new designs.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **Model Config Editor**.

Step 2 Click the **Discovery** tab.

A list of discovered devices that are available in the **Inventory** window is displayed.

Step 3 Click the radio button next to the device name and click **Discover Model Configs**.

Step 4 In the right pane, expand **Wireless** and choose a model configuration design type.

The configuration available for the selected model configuration type is displayed. For example, if you choose **CleanAir Configuration** under **Wireless**, the available configuration for the CleanAir is displayed.

Step 5 Click the radio button next to the configuration that you want to use as a template to create a new design, and click **Create Design**.

Step 6 In the window that is displayed, make the necessary changes and click **Save**.

Create a Model Config Design for AAA RADIUS Attributes

Use the **AAA Radius Attributes Configuration** model configuration design to define the Called-station-id parameter value for Cisco AireOS Wireless Controllers and Cisco Catalyst 9800 Series Wireless Controllers.

The **Default AAA_Radius_Attributes_Configuration** defines the called-station ID as **ap-macaddress-ssid**. You cannot edit or delete this default model configuration design. However, you can create a custom model configuration design for your specific network design.

Before you begin

You should have discovered the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **Model Config Editor**.

Step 2 In the left pane, expand **Wireless** and choose **AAA Radius Attributes Configuration**.

Alternatively, you can search for a model configuration by entering its name in the **Search** field.

Step 3 In the **Design Instances** window, click **Add**.

Step 4 In the **Design Name** field of the **Add Called-station-id** slide-in pane, enter a name for the model configuration design.

Step 5 To lock all the properties in the design, click **Lock all**. To lock a specific property, click the corresponding lock icon next to the property.

A property that is locked in the design can't be changed during device provisioning.

Step 6 From the **Called-station-id** drop-down list, choose an attribute value.

Step 7 Click **Save**.

The new design instance is displayed in the **Design Instances** window.

Step 8 (Optional) To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

What to do next

1. Attach the created model configuration design to a network profile so that it can be deployed on a wireless controller. From the top-left corner, click the menu icon and choose **Design** > **Network Profiles**. For more information, see Create Network Profiles for Wireless.
2. Provision the model configuration design specified in the network profile to network devices. From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**. For more information, see Provision a Cisco AireOS Controller or Provision a Cisco Catalyst 9800 Series Wireless Controller.

Create a Model Config Design for Advanced SSID

A WLAN associates an service set identifier (SSID) to an interface or an interface group. The WLAN is configured with security, quality of service (QoS), radio policies, and other wireless network parameters. You can configure up to 512 WLANs for each wireless controller.

Use the **Advanced SSID Configuration** model configuration design to configure the advanced SSID parameters on devices.

Before you begin

You must discover the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **Model Config Editor**.

Step 2 In the left pane, expand **Wireless** and choose **Advanced SSID Configuration**.

Alternatively, you can search for a model configuration by entering its name in the **Search** field.

Step 3 In the **Design Instances** window, check the **Default Advanced SSID Design** check box to use the default advanced SSID design.

Note You can't edit or delete the **Default Advanced SSID Design**.

Step 4 In the **Design Instances** window, click **Add**.

Step 5 In the **Design Name** field of the **Add Advanced SSID Configuration** slide-in pane, enter a name for the model configuration.

Step 6 To lock all the properties in the design, click **Lock all**. To lock a specific property, click the corresponding lock icon next to the property.

A property that is locked in the design can't be changed during device provisioning.

Step 7 In the **General** tab, do the following:

a) From the **Peer to Peer Blocking** drop-down list, choose an option for peer-to-peer blocking.

Peer-to-peer blocking is applied to individual WLANs. Each client inherits the peer-to-peer blocking setting of the WLAN to which it's associated. Peer-to-peer blocking enables you to have more control over how traffic is directed.

- **DISABLE**: Disables peer-to-peer blocking and forwards traffic locally within the wireless controller whenever possible.
- **DROP**: Causes the wireless controller to discard the client packets.
- **FORWARD UP**: Causes the client packets to be forwarded on an upstream VLAN. The device above the wireless controller decides what to do with the packets. The device can either be a router or a Layer 3 switch.
- **ALLOW PVT GROUP**: Applicable to preshared key (PSK) clients only. Traffic is forwarded based on the associated identity PSK (IPSK) tags for the source and destination client devices.

b) Click the **Passive Client Enable** toggle button to enable the Passive Client feature.

Passive clients are wireless devices, such as scales and printers, that are configured with a static IP address. These clients do not transmit any IP information (such as IP address, subnet mask, and gateway information) when they associate with an AP. As a result, when passive clients are used, the wireless controller never knows the IP address unless they use DHCP.

c) Click the **Assisted Roaming Prediction Optimization** toggle button to configure an assisted roaming prediction list for a WLAN.

d) Click the **Neighbor List Dual Band** toggle button to configure a neighbor list on a dual radio band.

e) Click the **Network Admission Control (NAC-SNMP)** toggle button to enable SNMP NAC support on the WLAN.

f) Click the **Network Admission Control (NAC-Radius)** toggle button to enable RADIUS NAC support on the WLAN.

g) From the **DHCP Required** drop-down list, choose **Yes** or **No** to pass the DHCP request before going into the RUN state (a state where the client can pass traffic through the wireless controller).
h) In the **DHCP Server - IP Address** field, enter the IP address of the DHCP server.
i) Click the **FlexConnect Local Authentication** toggle button to enable FlexConnect local authentication.
j) Click the **802.11ax Status** toggle button to enable 802.11ax configuration parameters.
k) Click the **Aironet IE** toggle button to enable support for Aironet IE on this SSID.
l) Click the **Load Balance Enable** toggle button to enable the load balancing feature.
m) In the **DTIM Period 5GHz Band (In Beacon Intervals) [1-255]** field, enter a value for the 5-GHz band.

   The valid range is from 1 through 255. The default value is 1 (to transmit broadcast and multicast frames after every beacon).

   If the beacon period of the 802.11 network is 100 ms and the DTIM value is set to 1, the AP transmits buffered broadcast and multicast frames 10 times every second. If the beacon period is 100 ms and the DTIM value is set to 2, the AP transmits buffered broadcast and multicast frames five times every second. Either of these settings are suitable for applications, including Voice Over IP (VoIP), that expect frequent broadcast and multicast frames.

   However, the DTIM value can be set as high as 255 (to transmit broadcast and multicast frames after every 255th beacon).

n) In the **DTIM Period 2.4GHz Band (In Beacon Intervals) [1-255]** field, enter a value for the 2.4-GHz band. The valid range is from 1 through 255. The default value is 1 (to transmit broadcast and multicast frames after every beacon).
o) In the **Max Clients Per WLAN** field, enter the maximum number of clients that are allowed to join the WLAN.

   The valid range is between 0 and 10,000.

p) In the **Max Clients Per AP Radio Per WLAN [0-500]** field, enter the maximum number of clients that are allowed to join the WLAN per AP.

   The valid range is between 0 and 500.

q) In the **Max Clients Per AP Per WLAN [0-1200]** field, enter the maximum number of client connections that are allowed per AP.

   The valid range is between 0 and 1200.

r) From the **WMM Policy** drop-down list, choose an option for the WMM policy: **Allowed**, **Disabled**, or **Required**.

   By default, the WMM policy is **Allowed**.

s) In the **NAS ID** field, enter the network access server identifier.

Step 8 In the **Client Data Rates** tab, configure the following client data rate limits per client by entering values in the respective fields:

- **Average Downstream Data Rate Per Client (kbps)**
- **Burst Downstream Data Rate Per Client (kbps)**
- **Average Downstream Real-Time Rate Per Client (kbps)**
- **Burst Downstream Real-Time Rate Per Client (kbps)**
- **Average Upstream Data Rate Per Client (kbps)**
- **Burst Upstream Data Rate Per Client (kbps)**
- **Average Upstream Real-Time Rate Per Client (kbps)**

- **Burst Upstream Real-Time Rate Per Client (kbps)**

Step 9 In the **SSID Data Rates** tab, configure the following SSID data rate limits per SSID by entering values in the respective fields:

- **Average Upstream Data Rate Per SSID (kbps)**
- **Burst Upstream Data Rate Per SSID (kbps)**
- **Average Upstream Real-Time Rate Per SSID (kbps)**
- **Burst Upstream Real-Time Rate Per SSID (kbps)**
- **Average Downstream Data Rate Per SSID (kbps)**
- **Burst Downstream Data Rate Per SSID (kbps)**
- **Average Downstream Real-Time Rate Per SSID (kbps)**
- **Burst Downstream Real-Time Rate Per SSID (kbps)**

Step 10 Hover your cursor over **More** and click **802.11ax Configuration** to configure the 802.11ax BSS configuration parameters. To enable or disable the following parameters, you can use the corresponding toggle buttons:

- **BSS Target Wake Up Time**
- **Downlink OFDMA**
- **Uplink OFDMA**
- **Downlink MU-MIMO**
- **Uplink MU-MIMO**

Note These parameters apply only to 2.4-GHz and 5-GHz radio bands. You can configure 802.11ax parameters for the 6-GHz radio band under the **Design** > **Network Settings** > **Wireless** > **RF Profiles** window. For more information, see Create a Wireless Radio Frequency Profile.

Step 11 Hover your cursor over **More** and click **Off Channel Scanning Defer** to configure the scan defer time and defer priority.

a) In the **Scan Defer Time [0-60000msecs]** field, set the time in milliseconds.

The valid values are between 0 and 60000 milliseconds; the default value is 100 milliseconds. If you set the time to 0, the scan deferral does not happen. The scan defer time is common for all priorities on the same WLAN, and the scan is deferred if a packet is transmitted or received in any one of the deferred priorities.

b) Click the corresponding toggle buttons to configure the required priority markings for packets:

- **Defer Priority0**
- **Defer Priority1**
- **Defer Priority2**
- **Defer Priority3**
- **Defer Priority4**
- **Defer Priority5**

- **Defer Priority6**
- **Defer Priority7**

Note These parameters are not supported on the Cisco AireOS Wireless Controller.

Step 12 Hover your cursor over **More** and click **Device Analytics** to configure the device analytics parameters:

a) Click the **Share Data with Client** toggle button to enable sharing Cisco device data with the client.
b) Click the **Advertise Support** toggle button to configure device analytics support.
c) Click the **Advertise PC Analytics Support** toggle button to configure PC analytics support.

Note These parameters are not supported on the Cisco AireOS Wireless Controller.

Step 13 Hover your cursor over **More** and click **802.11k Beacon Radio Measurement** to configure the 802.11k beacon radio measurement parameters:

a) Click the **Client Scan Report On Association** toggle button to send beacon measurement request (client scan report) on client association.
b) Click the **Client Scan Report On Roam** toggle button to send beacon measurement request (client scan report) on client roaming.

Note These parameters are not supported on the Cisco AireOS Wireless Controller.

Step 14 Hover your cursor over **More** and click **Multicast Buffer** to configure the multicast buffer parameter:

a) Click the **Multicast Buffer Enable** toggle button to configure multicast buffer tuning mode for 802.11a radio for WLAN.

Note This parameter is not supported on the Cisco AireOS Wireless Controller.

Step 15 Hover your cursor over **More** and click **SIP-CAC** to configure the SIP Call Admission Control (CAC) parameters:

a) Click the **Call Snooping** toggle button to configure call snooping for the WLAN mapped to the policy profile.
b) Click the **Send Disassociate** toggle button to configure the SIP CAC send disassociate option.
c) Click the **Send 486 Busy** toggle button to configure the SIP CAC send 486 busy option.

Note These parameters are not supported on the Cisco AireOS Wireless Controller.

Step 16 Hover your cursor over **More** and click **Miscellaneous** to configure the following parameters:

a) Click the **Media Stream Multicast-Direct** toggle button to configure multicast direct for WLAN.
b) Click the **802.11ac MU-MIMO** toggle button to configure 802.11ac MU-MIMO on WLAN.
c) Click the **Wifi To Cellular Steering** toggle button to configure WiFi to cellular steering on WLAN.
d) Click the **Wi-Fi Alliance Agile Multiband** toggle button to configure WiFi alliance agile multiband (MBO) support.
e) Click the **Fastlane+ (ASR)** toggle button to configure advanced scheduling request handling on WLAN.
f) Click the **Dot11v Bss Max Idle Protected** toggle button to configure BSS maximum idle processing per WLAN.
g) Click the **Universal Admin** toggle button to allow universal admin mode to be enabled on a 802.1x, WPA, or WPA2-secured WLAN.
h) Click the **Opportunistic Key Caching** toggle button to configure opportunistic key caching.
i) Click the **IP Source Guard** toggle button to configure MAC verification.
j) Click the **Enable DHCP Option82 Remote ID suboption** toggle button to configure the DHCP Option82 remote ID option.
k) Click the **VLAN Central Switching** toggle button to configure VLAN central switching.

l) Click the **IP Mac Binding** toggle button to configure control over support for IP MAC binding creation.
m) In the **Idle threshold(0-4294967295 bytes)** field, enter the idle threshold value. The valid range is between 0 and 4294967295 bytes. The default value is 0.
n) In the **Reassociation Timeout time [1-100 seconds]** field, enter the reassociation timeout time. The valid range is between 1 and 100 seconds. The default value is 20 seconds.
o) From the **mDNS Mode** drop-down list, choose an mDNS mode: **Bridging**, **Drop**, or **Gateway**

Note These parameters are not supported on the Cisco AireOS Wireless Controller.

Step 17 Click **Save**.

The created design instance is displayed in the **Design Instances** window under the **Advanced SSID Configuration - Model Configs** area.

Step 18 (Optional) To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

What to do next

1. Attach the created model configuration design to a network profile so that it can be deployed on the wireless controller. From the top-left corner, click the menu icon and choose **Design** > **Network Profiles**. For more information, see Create Network Profiles for Wireless.
2. Provision the model configuration design specified in the network profile to network devices. From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**. For more information, see Provision a Cisco AireOS Controller.

Create a Model Config Design for Cisco CleanAir

CleanAir is a spectrum intelligence solution designed to manage the challenges of a shared wireless spectrum proactively. It allows you to see all the users of the shared spectrum (both native devices and foreign interferers). It also enables you or your network to act on this information. For example, you can manually remove the interfering device, or the system can automatically steer the channel away from the interference. CleanAir provides spectrum management and Radio Frequency (RF) visibility.

Before you begin

You should have discovered the devices in your network using the **Discovery** functionality so that the discovered devices are listed in the **Inventory** window.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **Model Config Editor**.

Step 2 In the left pane, expand **Wireless** and choose **CleanAir Configuration**.

Alternatively, you can search for a model configuration by entering its name in the **Search** field.

Step 3 In the **Design Instances** window, check the **Default CleanAir 802.11a Design** or **Default CleanAir 802.11b Design** check box to use the default CleanAir design.

Note You can't edit and delete the **Default CleanAir 802.11a Design** or **Default CleanAir 802.11b Design**.

Step 4 In the **Design Instances** window, click **Add**.

Step 5 In the **Design Name** field of the **Add CleanAir Configuration** window, enter a name for the design.

Step 6 To lock all the properties in the design, click **Lock all**. To lock a specific property, click the corresponding lock icon next to the property.

A property that is locked in the design can't be changed during device provisioning.

Step 7 From the **Radio Band** drop-down list, choose **2.4 GHz** or **5 GHz**.

Step 8 Click the **CleanAir Enable** toggle button to enable the CleanAir functionality on the 2.4-GHz or 5-GHz radio band.

If the **CleanAir Enable** toggle button is enabled, click it to disable the feature and prevent the wireless controller from detecting spectrum interference.

Step 9 Click the **CleanAir Device Reporting Enable** toggle button to enable the CleanAir system to report detected sources of interference, if any.

If the **CleanAir Device Reporting Enable** toggle button is enabled, click it to disable the feature and prevent the wireless controller from reporting interferers.

Step 10 Click the **Persistent Device Propagation** toggle button 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 APs that are connected to the same wireless controller. Persistent interferers are present at the location, and interfere with WLAN operations even if they are not detectable at all times.

Step 11 Expand **Enable Interferers Features** and check the check box next to the source of interference that needs to be detected and reported by the CleanAir system:

- Ble Beacon
- Bluetooth Paging Inquiry
- Bluetooth SCO ACL
- Generic Dect
- Generic TDD
- Generic Waveform
- Jammer
- Microwave Oven
- Motorola Canopy
- SI FHSs
- Spectrum 802.11 FH
- Spectrum 802.11 Non STD Channel
- Spectrum 802.11 Spec Inverted
- Spectrum 802.11 Super AG SuperAG
- Spectrum 802.15.4
- Video

- Wimax Fixed
- Wimax Mobile
- Xbox

Step 12 In the **CleanAir Description** field, enter a description.

Step 13 Click **Save**.
The created design instance is displayed in the **Design Instances** window under the **CleanAir Configuration - Model Configs** area.

Step 14 (Optional) To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

What to do next

1. Attach the created model configuration design to a network profile so that it can be deployed on the wireless controller. From the top-left corner, click the menu icon and choose **Design** > **Network Profiles**. For more information, see Create Network Profiles for Wireless.
2. Provision the model configuration design specified in the network profile to network devices. From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**. For more information, see Provision a Cisco AireOS Controller.

Create a Model Config Design for Dot11ax Configuration

The **Dot11ax Configuration** model configuration design configures Dot11ax parameters on devices.

The Dot11ax configuration involves the 802.11ax wireless specifications standard, also known as High Efficiency (HE) Wireless. Dot11ax is a dual-band technology that uses 2.4-GHz, 5-GHz, and 6-GHz bands. You can configure Dot11ax configuration parameters only on Wi-Fi 6-supported Cisco Catalyst 9100 Series Access Points.

Note BSS color is used to identify an overlapping basic service set (OBSS). BSS configurations are pushed on Wi-Fi 6-supported APs only. The Cisco Catalyst 9100 Series Access Points are the next-generation Wi-Fi 802.11ax APs, and ideal for high-density, high-definition applications.

Before you begin

You must discover the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **Model Config Editor**.

Step 2 In the left pane, expand **Wireless** and choose **Dot11ax Configuration**.

Alternatively, you can search for a model configuration by entering its name in the **Search** field.

Step 3 In the **Design Instances** window, to use the default Dot11ax designs, check the check box next to the required default designs:

- **Default Dot11ax 6-GHz Design**
- **Default Dot11ax 802.11a Design**
- **Default Dot11ax 802.11b Design**

Note You can't edit or delete the default Dot11ax designs.

Step 4 In the **Design Instances** window, click **Add**.

Step 5 In the **Design Name** field of the **Add Dot11ax Configuration** window, enter a name for the model configuration design.

Step 6 To lock all the properties in the design, click **Lock all**. To lock a specific property, click the corresponding lock icon next to the property.

A property that is locked in the design can't be changed during device provisioning.

Step 7 Click the **BSS Color** toggle button to enable the BSS color functionality. The default value is disabled.

BSS color functionality is supported on:

- Cisco AireOS Wireless Controllers that run Cisco AireOS Release 8.10 and later
- Cisco Wireless Controllers that run Cisco IOS XE Release 17.1 and later

Step 8 Click the **Target Wakeup Time** toggle button to enable the target wake-up time. The default value is disabled.

Target wake-up time is supported on:

- Cisco AireOS Wireless Controllers that run Cisco AireOS Release 8.10 and later
- Cisco Wireless Controllers that run Cisco IOS XE Release 17.1 and later

Step 9 Click the **Target Wakeup Time Broadcast** toggle button to enable the target wake-up time broadcast. The default value is disabled.

Target wake-up time broadcast is supported on:

- Cisco AireOS Wireless Controllers that run Cisco AireOS Release 8.10 and later
- Cisco Wireless Controllers that run Cisco IOS XE Release 17.3.1 and later

Step 10 Click the **Multiple BSSID** toggle button to enable the multiple basic service set identifier (BSSID) functionality. The default value is disabled.

Multiple BSSID is supported only on Cisco Wireless Controllers that run Cisco IOS XE Release 17.7.1 and later.

Note This toggle button is available only when you choose the **6 GHz** radio band.

Step 11 From the **Radio Band** drop-down list, choose **2.4 GHz**, **5 GHz**, or **6 GHz**. The default value is disabled.

Step 12 Click the **OBSS PD** toggle button to enable the Overlapping BSS Packet Detect (OBSS-PD) functionality.

OBSS-PD is supported only on Cisco Wireless Controllers that run Cisco IOS XE Release 17.4 and later.

Note This toggle button is not available for the **6 GHz** radio band.

Step 13 In the **Non-SRG OBSS PD Max Threshold (dbm)** field, enter a value for the non-Spatial Reuse Group (SRG) OBSS-PD maximum threshold in dBm. The default value is -62 dBm.

Non-SRG OBSS-PD is supported only on Cisco Wireless Controllers that run Cisco IOS XE Release 17.4 and later.

Note This toggle button is not available for the **6 GHz** radio band.

Step 14 Click **Save**.

The created design instance is displayed in the **Design Instances** window under the **Dot11ax Configuration – Model Configs** area.

Step 15 (Optional) To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

What to do next

1. Attach the created model configuration design to a network profile so that it can be deployed on the APs. From the top-left corner, click the menu icon and choose **Design** > **Network Profiles**. For more information, see Create Network Profiles for Wireless.
2. Provision the model configuration design specified in the network profile to network devices. From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**. For more information, see Provision a Cisco AireOS Controller.

Create a Model Config Design for Event-Driven RRM

The **Event Driven RRM Configuration** model configuration design configures event-driven RRM parameters for the 2.4-GHz, 5-GHz, and 6-GHz radios.

Before you begin

You should have discovered the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **Model Config Editor**.

Step 2 In the left pane, expand **Wireless** and choose **Event Driven RRM Configuration**.

Alternatively, you can search for a model configuration by entering its name in the **Search** field.

Step 3 In the **Design Instances** window, check the **Default Event Driven 2.4GHz Design** or **Default Event Driven 5 GHz Design** check box to use the default advanced SSID design.

Note You can’t edit or delete the default event-driven RRM design.

Step 4 In the **Design Instances** window, click **Add**.

Step 5 In the **Design Name** field of the **Add Event Driven RRM Configuration** slide-in pane, enter a name for the model configuration design.

Step 6 To lock all the properties in the design, click **Lock all**. To lock a specific property, click the corresponding lock icon next to the property.

A property that is locked in the design can't be changed during device provisioning.

Step 7 From the **Radio Band** drop-down list, select the radio band: **2.4GHz**, **5GHz**, or **6GHz**.

Note The 6-GHZ radio band is not supported on Cisco AireOS Wireless Controllers.

Cisco Catalyst 9800 Series Wireless Controllers running Cisco IOS XE Release 17.6 and later support the 6-GHz radio band.

Step 8 Click the **Event Driven RRM** toggle button to run RRM when a CleanAir-enabled AP detects a significant level of interference.

Step 9 From the **Sensitivity Threshold** drop-down list, choose the sensitivity threshold level at which you want the RRM to be triggered from the following options.

When the interference for the AP rises above the threshold level, RRM initiates a local dynamic channel assignment (DCA) run and changes the channel of the affected AP radio, if possible, to improve network performance.

- **Low**: Specifies the least sensitivity to non-Wi-Fi interference as indicated by the AQ value.
- **Medium**: Specifies medium sensitivity to non-Wi-Fi interference as indicated by the AQ value.
- **High**: Specifies the most sensitivity to non-Wi-Fi interference as indicated by the AQ value.
- **Custom**: Specifies custom sensitivity to non-Wi-Fi interference as indicated by the AQ value. If you choose this option, you must specify a custom value in the **Custom Threshold [1-99]** field.

Step 10 Click **Save**.

The created design instance is displayed in the **Design Instances** window under the **Event Driven RRM Configuration - Model Configs** area.

Step 11 (Optional) To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

What to do next

1. Attach the created model configuration design to a network profile so that it can be deployed on the wireless controller. From the top-left corner, click the menu icon and choose **Design** > **Network Profiles**. For more information, see Create Network Profiles for Wireless.
2. Provision the model configuration design specified in the network profile to network devices. From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**. For more information, see Provision a Cisco AireOS Controller.

Create a Model Config Design for Flex Configuration

Use the **Flex Configuration** model configuration design to configure the FlexConnect configuration on devices.

Before you begin

Using the **Discovery** feature, discover the devices in your network so that the discovered devices are listed in the **Inventory** window.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **Model Config Editor**.

Step 2 In the left pane, expand **Wireless** and choose **Flex Configuration**.

Alternatively, you can search for a model configuration by entering its name in the **Search** field.

Step 3 In the **Design Instances** window, check the **Default Flex Configuration** check box to use the default FlexConnect design.

Note You can't edit or delete the **Default Flex Configuration** design.

Step 4 In the **Design Instances** window, click **Add**.

Step 5 In the **Design Name** field of the **Add Flex Configuration** slide-in pane, enter a name for the design.

Step 6 To lock all the properties in the design, click **Lock all**. To lock a specific property, click the corresponding lock icon next to the property.

A property that is locked in the design can’t be changed during device provisioning.

Step 7 From the **Radio Band** drop-down list, choose **2.4 GHz** or **5 GHz**.

Step 8 Click the **CleanAir Enable** toggle button to enable the CleanAir functionality on the 2.4-GHz or 5-GHz radio band.

If the **CleanAir Enable** toggle button is enabled, click it to prevent the Cisco Wireless Controller from detecting spectrum interference.

Step 9 Click the **CleanAir Device Reporting Enable** toggle button to enable the CleanAir system to report detected sources of interference, if any.

If the **CleanAir Device Reporting Enable** toggle button is enabled, click it to prevent the Cisco Wireless Controller from reporting interferers.

Step 10 Click the **Persistent Device Propagation** toggle button 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 APs that are connected to the same Cisco Wireless Controller. Persistent interferers are present at the location, and interfere with WLAN operations even if they are not detectable at all times.

Step 11 Expand **Enable Interferers Features** and check the check box next to the source of interference that needs to be detected and reported by the CleanAir system:

- Ble Beacon
- Bluetooth Paging Inquiry
- Bluetooth SCO ACL
- Generic Dect
- Generic TDD
- Generic Waveform

- Jammer
- Microwave Oven
- Motorola Canopy
- SI FHSs
- Spectrum 802.11 FH
- Spectrum 802.11 Non STD Channel
- Spectrum 802.11 Spec Inverted
- Spectrum 802.11 Super AG SuperAG
- Spectrum 802.15.4
- Video
- Wimax Fixed
- Wimax Mobile
- Xbox

Step 12 In the **CleanAir Description** field, enter a description.

Step 13 Click **Apply**.
The created design instance is displayed in the **Design Instances** window under the **CleanAir Configuration - Model Configs** area.

Step 14 (Optional) To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

What to do next

1. Attach the created model configuration design to a network profile so that it can be deployed on the wireless controller. From the top-left corner, click the menu icon and choose **Design** > **Network Profiles**. For more information, see Create Network Profiles for Wireless.
2. Provision the model configuration design specified in the network profile to network devices. From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**. For more information, see Provision a Cisco AireOS Controller.

Create a Model Config Design for Global IPv6 Configuration

Before you begin

You should have discovered the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **Model Config Editor**.

Step 2 In the left pane, expand **Wireless** and choose **Global IPV6 Configuration**.

Alternatively, you can search for a model configuration by entering its name in the **Search** field.

Step 3 In the **Design Instances** window, check the **Default Global IPv6 Design** check box to use the default global IPV6 design.

Note You can't edit or delete the **Default Global IPv6 Design**.

Step 4 In the **Design Instances** window, click **Add**.

The window appears.

Step 5 In the **Design Name** field of the **Add Global IPV6 Configuration** slide-in pane, enter a name for the model configuration design.

Step 6 To lock all the properties in the design, click **Lock all**. To lock a specific property, click the corresponding lock icon next to the property.

A property that is locked in the design can't be changed during device provisioning.

Step 7 Click the **Global IPV6 Config** toggle button to enable IPv6 globally on devices.

Step 8 Click **Save**.

The created design instance is displayed in the **Design Instances** window under the **Global IPV6 Configuration - Model Config** area.

Step 9 (Optional) To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

What to do next

1. Attach the created model configuration design to a network profile so that it can be deployed on the wireless controller. From the top-left corner, click the menu icon and choose **Design** > **Network Profiles**. For more information, see Create Network Profiles for Wireless.
2. Provision the model configuration design specified in the network profile to network devices. From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**. For more information, see Provision a Cisco AireOS Controller.

Create a Model Config Design for Multicast

Use the **Multicast Configuration** model configuration design to configure multicast parameters on devices.

If your network supports packet multicasting, you can configure the multicast method that the Cisco Wireless Controller uses. The wireless controller performs multicasting in one of these modes:

- Unicast mode: In this mode, the wireless controller unicasts every multicast packet to every access point associated to the wireless controller. This mode is not very efficient, but is required on networks that do not support multicasting.
- Multicast mode: In this mode, the wireless controller sends multicast packets to a CAPWAP multicast group. This method reduces the overhead on the wireless controller processor and shifts the work of packet replication to your network. This method is more efficient than the unicast method.

Before you begin

You should have discovered the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **Model Config Editor**.

Step 2 In the left pane, expand **Wireless** and choose **Multicast Configuration**.

Alternatively, you can search for a model configuration by entering its name in the **Search** field.

Step 3 In the **Design Instances** window, check the **Default Multicast Design** check box to use the default multicast design.

Note You can't edit or delete **Default Multicast Design**.

Step 4 In the **Design Instances** window, click **Add Design**.

Step 5 In the **Design Name** field of the **Add Multicast Configuration**, enter a name for the model configuration design.

Step 6 To lock all the properties in the design, click **Lock all**. To lock a specific property, click the corresponding lock icon next to the property.

A property that is locked in the design can’t be changed during device provisioning.

Step 7 Click the **Enable Global Multicast Mode** toggle button to configure sending multicast packets. The default value is disabled.

Step 8 From the **AP Multicast Mode** drop-down list, choose **UNICAST** or **MULTICAST**.

- Choose **UNICAST** to configure the wireless controller to use the unicast method to broadcast packets.
- Choose **MULTICAST** to configure the wireless controller to use the multicast method to broadcast packets to a CAPWAP multicast group.

Step 9 Expand **IPV4 Multicast Group Address** and enter the IPv4 multicast address in the **IP Address** field.

Step 10 Expand **IPV6 Multicast Group Address** and enter the IPv6 multicast address in the **IP Address** field.

Step 11 Click **Apply**.

The created design instance is displayed in the **Design Instances** window under the **Multicast - Model Config** area.

Step 12 (Optional) To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

What to do next

1. Attach the created model configuration design to a network profile so that it can be deployed on the wireless controller. From the top-left corner, click the menu icon and choose **Design** > **Network Profiles**. For more information, see Create Network Profiles for Wireless.
2. Provision the model configuration design specified in the network profile to network devices. From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**. For more information, see Provision a Cisco AireOS Controller.

Create a Model Config Design for RRM FRA Parameters

The **RRM FRA Configuration** model configuration design configures the Flexible Radio Assignment (FRA) parameters for Radio Resource Management (RRM) for 2.4-5 GHz and 5-6 GHz radio bands.

Before you begin

You must discover the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **Model Config Editor**.

Step 2 In the left pane, expand **Wireless** and choose **RRM FRA Configuration**.

Alternatively, you can search for a model configuration by entering its name in the **Search** field.

Step 3 In the **Design Instances** window, check the corresponding default FRA design check box to use the default design:

- **Default FRA 2.4-5GHz Design**
- **Default FRA 5-6GHz Design**

Note
- You can't edit or delete the default FRA designs.
- The 6-GHz radio band is not supported in Cisco AireOS Wireless Controllers.
- The Cisco Catalyst 9800 Series Wireless Controllers that run Cisco IOS XE Release 17.6 and later support the 6-GHz radio band.

Step 4 In the **Design Instances** window, click **Add**.

Step 5 In the **Design Name** field of the **Add Flexible Radio Assignment (FRA) Configuration** slide-in pane, enter a name for the model configuration.

Step 6 To lock all the properties in the design, click **Lock all**. To lock a specific property, click the corresponding lock icon next to the property.

A property that is locked in the design can’t be changed during device provisioning.

Step 7 From the **Radio Band** drop-down list, choose a radio band.

Step 8 Click the **FRA Freeze** toggle button to enable the FRA freeze functionality. This functionality is disabled by default.

Cisco Wireless Controllers that run Cisco IOS XE Release 17.6.1 and later support this functionality.

Note This toggle button is available only for the **2.4-5 GHz** radio band.

Step 9 Click the **FRA Status** toggle button to enable the FRA status functionality. This functionality is enabled by default.

Step 10 From the **FRA Interval** drop-down list, choose an FRA interval.

Step 11 From the **FRA Sensitivity** drop-down list, choose an FRA sensitivity value.

This parameter sets the FRA coverage overlap sensitivity.

Note This drop-down list is available only for the **2.4-5 GHz** radio band.

Step 12 Click **Save**.

The created design instance is displayed in the **Design Instances** window in the **RRM FRA Configuration – Model Configs** area.

Step 13 (Optional) To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

What to do next

1. Attach the created model configuration design to a network profile so that it can be deployed on the access points. From the top-left corner, click the menu icon and choose **Design** > **Network Profiles**. For more information, see Create Network Profiles for Wireless.
2. Provision the model configuration design specified in the network profile to network devices. From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**. For more information, see Provision a Cisco AireOS Controller and Provision a Cisco Catalyst 9800 Series Wireless Controller.

Create a Model Config Design for RRM General Parameters

The **RRM General Configuration** model configuration design configures the Radio Resource Management (RRM) general parameters for the 2.4-GHz, 5-GHz, and 6-GHz radios.

Before you begin

You should have discovered the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **Model Config Editor**.

Step 2 In the left pane, expand **Wireless** and choose **RRM General Configuration**.

Alternatively, you can search for a model configuration by entering its name in the **Search** field.

Step 3 The **Design Instances** window shows the following default RRM general configuration designs. You can check the respective default **RRM General Design** check box to use the default design.

You can't edit or delete the Default RRM General Design.

- Default RRM General 2.4 GHz Design
- Default RRM General 5 GHz Design
- Default RRM General 6 GHz Design

Note The 6-GHz radio band is not supported on Cisco AireOS Wireless Controllers.

Note Cisco Catalyst 9800 Series Wireless Controller running Cisco IOS XE Release 17.6 and later releases support the 6-GHz radio band.

Step 4 In the **Design Instances** window, click **Add**.

Step 5 In the **Design Name** field of the **Add RRM General Configuration** slide-in pane, enter a name for the model configuration design.

Step 6 To lock all the properties in the design, click **Lock all**. To lock a specific property, click the corresponding lock icon next to the property.

A property that is locked in the design can't be changed during device provisioning.

Step 7 In the **Radio Band** tab, choose the radio band from the **Radio Band** drop-down list: **2.4 GHz**, **5 GHz**, or **6 GHz**.

Step 8 In the **Threshold** tab, set the throughput threshold value for the radio band selected in the Throughput Threshold (1000-10000000 Bps) field.

Step 9 In the **Monitoring** tab, configure the monitoring channels and neighbor discover type.

- From the **Monitoring Channels** drop-down list, choose one of the following options to specify the set of channels that the AP uses for RRM scanning. By default, the monitoring channel is set to Country.
  - **All**: RRM channel scanning occurs on all channels supported by the selected radio, which includes channels not allowed in the country of operation.
  - **Country**: RRM channel scanning occurs only on the data channels in the country of operation. This is the default value.
  - **DCA**: RRM channel scanning occurs only on the channel set used by the DCA algorithm.
- From the **Neighbor Discover Type** drop-down list, choose the neighbor discovery type. By default, the mode is set to Transparent.
  - **Transparent**: Sets the neighbor discover type to transparent. Packets are sent as is.
  - **Protected**: Sets the neighbor discover type to protected. Packets are encrypted.

Step 10 In the **Coverage** tab, click the **Global Coverage Hole Detection Enabled** toggle button to enable coverage hole detection. By default, this value is selected.

If you enable coverage hole detection, the Cisco Wireless Controller automatically determines, based on data received from the APs, if any APs have clients that are potentially located in areas with poor coverage.

Step 11 Click **Save**.

The created design instance is displayed in the **Design Instances** window under the **RRM General Configuration - Model Configs** area.

Step 12 (Optional) To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

What to do next

1. Attach the created model configuration design to a network profile so that it can be deployed on the wireless controller. From the top-left corner, click the menu icon and choose **Design** > **Network Profiles**. For more information, see Create Network Profiles for Wireless.

2. Provision the model configuration design specified in the network profile to network devices. From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**. For more information, see Provision a Cisco AireOS Controller.

Create a Model Config Design for Rogue General Parameters

Use this procedure to configure Rogue general configuration and client exclusions policies.

Before you begin

You must discover the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **Model Config Editor**.

Step 2 In the left pane, expand **Wireless** and choose **Rogue General Configuration**.

Alternatively, you can search for a model configuration by entering its name in the **Search** field.

Step 3 In the **Design Instances** window, to use the default rogue general configuration designs, check the check box next to the required default designs:

- **Default Rogue General Configuration Critical**
- **Default Rogue General Configuration Custom**
- **Default Rogue General Configuration High**
- **Default Rogue General Configuration Low**

Step 4 Click **Add** to create new rogue general configuration profile.

The **Add Rogue General Configuration** slide-in pane is displayed.

Step 5 In the **Add Rogue General Configuration** slide-in pane, do the following:

a) In the **Design Name** field, enter a name for the model configuration design.
b) In the **General** tab, choose the **Rogue Detection Security Level** from the drop-down list.
c) In the Expiration timeout for Rogue APs field, enter the time in seconds for the chosen rogue detection security level as follows:

- **LOW**: If you choose low security level, expiration timeout must be 240 seconds.
- **HIGH**: If you choose high security level, expiration timeout must be 1200 seconds.
- **CRITICAL**: If you choose critical security level, expiration timeout must be 3600 seconds.
- **CUSTOM**: If you choose custom security level, expiration timeout must be between 240 to 3500 seconds.

d) Toggle the **Validate Rogue Clients against AAA** toggle button to validate the rogue clients.
e) Toggle the **Detect and Report Adhoc Networks** toggle button to report adhoc network.
f) Toggle the **Validate Rogue APs against AAA** toggle button to validate the rogue APs.

Note **Validate Rogue APs against AAA** toggle button and **Rogue Polling Interval (seconds)** field is only displayed if you select security level as custom.

g) In the **Rogue Polling Interval (seconds)** field, enter a valid rogue polling time interval in seconds.

The valid rogue polling interval value ranges from 60 to 86400 seconds.

h) In the **Rogue Detection Client Number Threshold** field, enter the valid threshold value between 0 to 256.
i) In the **Rogue Init Timer (seconds)** field, enter the time in seconds. The default value is 180 seconds.
j) In the **AP Authentication Alarm Threshold** field, enter a valid threshold value between 1 to 255.
k) Toggle the **Syslog Notification** toggle button to get notification, if any system logs are generated.
l) In the **MFP Key Refresh Interval (hours)** field, enter a valid time interval in hours, between 1 to 24.
m) (Optional) To lock all the properties in the design, click **Lock all**. To lock a specific property, click the corresponding lock icon next to the property.
n) Click **Save**.

Step 6 Provision the model config design specified in the network profile to network devices. From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**.

For more information, see Provision a Cisco AireOS Controller.

What to do next

1. (Optional) To add model configuration to a network profile, see Add Model Configurations to a Network Profile.
2. Provision the model config design specified in the network profile to network devices. From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**.

   For more information, see Provision a Cisco AireOS Controller.