



Design Model Configuration

- [Introduction to Model Config Editor, on page 1](#)
- [Create a Model Config Design for AAA RADIUS Attributes, on page 2](#)
- [Create a Model Config Design for Advanced SSID, on page 3](#)
- [Create a Design for Cisco CleanAir, on page 6](#)
- [Create a Model Config Design for Dot11ax Configuration, on page 7](#)
- [Create a Model Config Design for Multicast, on page 9](#)
- [Create a Design for Global IPv6, on page 10](#)
- [Discover and Create Designs from a Legacy Device, on page 11](#)

Introduction to Model Config Editor

Model Config allows you to define advanced customizations of the Cisco Validated Designs (CVD) 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

- Advanced SSID configuration
- CleanAir configuration
- Dot11ax Configuration
- Global IPv6 configuration
- Multicast configuration

Create a Model Config Design for AAA RADIUS Attributes

Use the **AAA Radius Attributes Configuration** model config to define the **Called-station-id** parameter value for Cisco AireOS 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 config. However, you can create a custom model config for your specific network design.

This procedure describes how to create a new **AAA Radius Attributes Configuration** model config.

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** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools > Model Config Editor**.
- Step 2** In the left pane, you can either search for a model config by entering its name in the **Search** field, or by expanding **Wireless** and choosing **AAA Radius Attributes Configuration**.
- Step 3** In the **Design Instances** window, click **Add**.
The **Add Called-station-id** slide-in pane appears.
- Step 4** In the **Design Name** field, enter a name for the model config design.
- Step 5** From the **Called-station-id** drop-down list, choose one of the following attribute values:
- **ap-ethmac-only**
 - **ap-ethmac-ssid**
 - **ap-group-name**
 - **ap-label-address**
 - **ap-label-address-ssid**
 - **ap-location**
 - **ap-macaddress**
 - **ap-macaddress-ssid**
 - **ap-name**
 - **ap-name-ssid**

- **ipaddress**
- **macaddress**
- **vlan-id**

- Step 6** Click **Save**.
The new design instance appears in the **Design Instances** window.
- Step 7** 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**.
- Step 8** Attach the created config design to a network profile so that it can be deployed on a wireless controller. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design > Network Profiles**.
For more information, see [Create Network Profiles for Wireless](#).
- Step 9** Provision the model config design specified in the network profile to network devices. In the Cisco DNA Center GUI, 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 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 service set identifier (SSID) model config to configure the advanced SSID parameters on devices.

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** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools > Model Config Editor**.
- Step 2** In the left pane, you can either search for a model config by entering its name in the **Search** field, or expand **Wireless** and choose **Advanced SSID Configuration**.
- Step 3** In the **Design Instances** pane, check the **Default Advanced SSID Design** check box to use the default advanced SSID design.
Note You cannot edit or delete the Default Advanced SSID Design.
- Step 4** In the **Design Instances** pane, click **Add Design**.
The **Add Advanced SSID Configuration** window appears.
- Step 5** In the **Design Name** field, enter a name for the model config.

- Step 6** In the General tab, click the **Peer-to-Peer Blocking** drop-down list and 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 is 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 action to take regarding 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.
- Step 7** 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 access point. As a result, when passive clients are used, the wireless controller never knows the IP address unless they use DHCP.
- Step 8** Click the **Assisted Roaming Prediction Optimization** toggle button to configure an assisted roaming prediction list for a WLAN.
- Step 9** Click the **Neighbor List Dual Band** toggle button to configure a neighbor list on a dual radio band.
- Step 10** Click the **Network Admission Control (NAC-SNMP)** toggle button to enable SNMP NAC support on the WLAN.
- Step 11** Click the **Network Admission Control (NAC-Radius)** toggle button to enable RADIUS NAC support on the WLAN.
- Step 12** 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).
- Step 13** Expand **DHCP Server** and enter the IP address of the DHCP server in the **IP Address** field.
- Step 14** Click the **FlexConnect Local Authentication** toggle button to enable FlexConnect local authentication.
- Step 15** In the **NAS ID** field, enter the network access server identifier.
- Step 16** Click **Client Data Rates** to 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 17** Click the **SSID Data Rates** to 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)

Note To lock all the properties in the design, click **Lock all**. To lock a specific property, click the lock symbol next to that property.

Step 18 Click **802.11ax Configuration** to configure the 802.11ax BSS Configuration parameters. You can use the toggle button to enable or disable the following configuration parameters:

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

Note To lock all the properties in the design, click **Lock all**. To lock a specific property, click the lock symbol next to that property.

Step 19 Click **Save**.

The created design instance appears in the **Design Instances** window under the **Advanced SSID Configuration - Model Config** area.

Step 20 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**.

Step 21 Attach the created config design to a network profile so that it can be deployed on the wireless controller. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design > Network Profiles**.

For more information, see [Create Network Profiles for Wireless](#).

Step 22 Provision the model config design specified in the network profile to network devices. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Network Devices > Inventory**.

For more information, see [Provision a Cisco AireOS Controller](#).

Create a Design for Cisco CleanAir

CleanAir is a spectrum intelligence solution designed to proactively manage the challenges of a shared wireless spectrum. 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** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools > Model Config Editor**.
- Step 2** In the left pane, you can either search for a model config capability by entering its name in the **Search Capability** field, or by expanding the **Wireless** Model Configs and choosing **CleanAir Configuration**.
- Step 3** In the **Design Instances** pane, check the **Default CleanAir 802.11a Design** or **Default CleanAir 802.11b Design** check box to use the default CleanAir design.
- Note** You cannot edit and delete the **Default CleanAir 802.11a Design** or **Default CleanAir 802.11b Design**.
- Step 4** In the **Design Instances** window, click **Add**.
The **Add CleanAir Configuration** window is displayed.
- Step 5** In the **Design Name** field, enter a name for the design.
- Step 6** From the **Radio Band** drop-down list, choose **2.4 GHz** or **5 GHz**.
- Step 7** 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 8** 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 9** 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 10** 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 11 In the **CleanAir Description** field, enter a description.

Step 12 Click **Apply**.

The created design instance appears in the **Design Instances** window under the **CleanAir Configuration - Model Configs** area.

Step 13 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**.

Step 14 Attach the created config design to a network profile so that it can be deployed on the wireless controller. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design > Network Profiles**.

For more information, see [Create Network Profiles for Wireless](#).

Step 15 Provision the model config design specified in the network profile to network devices. In the Cisco DNA Center GUI, 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 Cisco DNA Center Dot11ax model config feature configures Dot11ax parameters on devices.

Dot11ax configuration involves the 802.11ax wireless specifications standard, also known as High Efficiency (HE) Wireless. Dot11ax is a dual-band 2.4-GHz and 5-GHz technology. 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 configs are pushed on Wi-Fi 6-supported access points only. The Cisco Catalyst 9100 series Access Points are the next-generation Wi-Fi 802.11ax access point, 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** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools > Model Config Editor**.
- Step 2** In the left pane, you can either search for a model config by entering its name in the **Search Capability** field, or by expanding **Wireless** and choosing **Dot11ax Configuration**.
- Step 3** In the **Design Instances** pane, check the **Default Dot11ax Design** check box to use the default dot11ax design.
- Note** You cannot edit and delete the **Default dot11ax Design**.
- Step 4** In the **Design Instances** window, click **Add Design**.
The **Add Dot11ax Configuration** window appears.
- Step 5** In the **Design Name** field, enter a name for the model config design.
- Step 6** Click the **BSS Color** toggle button to enable the BSS color functionality on the 2.4-GHz or 5-GHz radio band. The default value is disabled.
- Step 7** Click the **Target Wakeup Time** toggle button to enable the target wakeup time. The default value is disabled.
- Step 8** From the **Radio Band** drop-down list, choose a 2.4-GHz or 5-GHz radio band.
- Note** To lock all the properties in the design, click **Lock all**. To lock a specific property, click the lock symbol that is next to each property.
- Step 9** Click **Save**.
The created design instance appears in the Design Instances window under the **Dot11ax Configuration – Model Configs** area.
- Step 10** 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**.
- Step 11** Attach the created config design to a network profile so that it can be deployed on the access points. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design > Network Profiles**. For more information, see [Create Network Profiles for Wireless](#).
- Step 12** Provision the model config design specified in the network profile to network devices. In the Cisco DNA Center GUI, 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 model config feature 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** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **Tools > Model Config Editor**.
- Step 2** In the left pane, you can either search for a model config by entering its name in the **Search Capability** field, or by expanding **Wireless** and choosing **Multicast Configuration**.
- Step 3** In the **Design Instances** pane, check the **Default Multicast Design** check box to use the default multicast design.
- Note** You cannot edit or delete the **Default Multicast Design**.
- Step 4** In the **Design Instances** window, click **Add Design**.
The **Add Multicast Configuration** window appears.
- Step 5** In the **Design Name** field, enter a name for the model config design.
- Step 6** Click the **Enable Global Multicast Mode** toggle button to configure sending multicast packets. The default value is disabled.
- Step 7** 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 8** Expand **IPV4 Multicast Group Address** and enter the IPv4 multicast address in the **IP Address** field.
- Step 9** Expand **IPV6 Multicast Group Address** and enter the IPv6 multicast address in the **IP Address** field.
- Step 10** Click **Apply**.
The created design instance appears in the **Design Instances** window under the **Multicast - Model Config** area.
- Step 11** 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**.

- Step 12** Attach the created config design to a network profile so that it can be deployed on the wireless controller. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design > Network Profiles**.
- For more information, see [Create Network Profiles for Wireless](#).
- Step 13** Provision the model config design specified in the network profile to network devices. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Network Devices > Inventory**.
- For more information, see [Provision a Cisco AireOS Controller](#).
-

Create a Design for Global IPv6

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** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools > Model Config Editor**.
- Step 2** In the left pane, you can either search for a model config by entering its name in the **Search Capability** field, or expand **Wireless** and choose **Global IPV6 Configuration**.
- Step 3** In the **Design Instances** pane, check the **Default Global IPv6 Design** check box to use the default global IPv6 design.
- Note** You cannot edit or delete the **Default Global IPv6 Design**.
- Step 4** In the **Design Instances** window, click **Add Design**.
- The **Add Global IPV6 Configuration** window appears.
- Step 5** In the **Design Name** field, enter a name for the model config.
- Step 6** Click the **Global IPV6 Config** toggle button to enable IPv6 globally on devices.
- Step 7** Click **Apply**.
- The created design instance appears in the **Design Instances** window under the **Global IPV6 Configuration - Model Config** area.
- Step 8** 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**.
- Step 9** Attach the created config design to a network profile so that it can be deployed on the wireless controller. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design > Network Profiles**.
- For more information, see [Create Network Profiles for Wireless](#).
- Step 10** Provision the model config design specified in the network profile to network devices. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Network Devices > Inventory**.
- For more information, see [Provision a Cisco AireOS Controller](#).
-

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 config designs available on legacy devices and use them as a template to create new designs.

-
- Step 1** In the Cisco DNA Center GUI, 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 appears.
- 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 config design type.
- The configuration available for the selected model config type appears. For example, if you choose **CleanAir Configuration** under **Wireless**, the available configuration for the CleanAir appears.
- 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 appears, make the necessary changes and click **Save**.
-

