cnPilot Recommended Base Configuration

Overview

This document provides a base set of configurations to be used in normal situations. This is only a recommendation from which to start and is not intended to fulfill the needs of every situation.

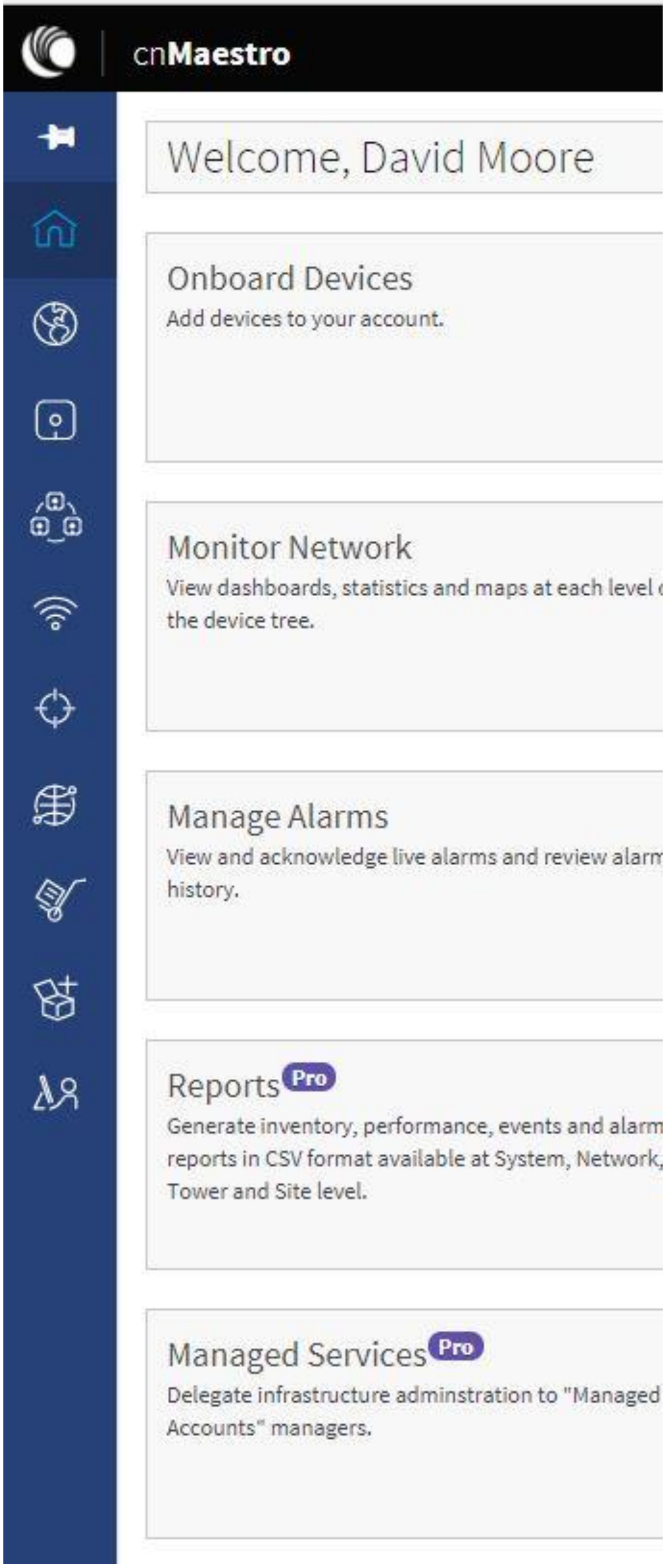
Contents

Configuration Methods

It is possible to configure cnPilot APs through three different methods: cnMaestro, the AP GUI itself, or AutoPilot. Of the three, the most common, and the most straight forward is via cnMaestro. This document will cover using both cnMaestro and the AP GUI. AutoPilot configuration is very similar to using cnMaestro and will not be addressed separately.

Configuring through cnMaestro

When using cnMaestro for the first time it can be confusing as to the order in which to configure each piece, be it the WLANs, the AP Groups, or even onboarding APs. The most intuitive route would seem to be to start at the top left and work your way down. Looking at the left hand side of the screen when you first log into cnMaestro you will see a menu with a blue background.



Welcome, David Moore

Onboard Devices
Add devices to your account.

Monitor Network
View dashboards, statistics and maps at each level
the device tree.

Manage Alarms
View and acknowledge live alarms and review alarm
history.

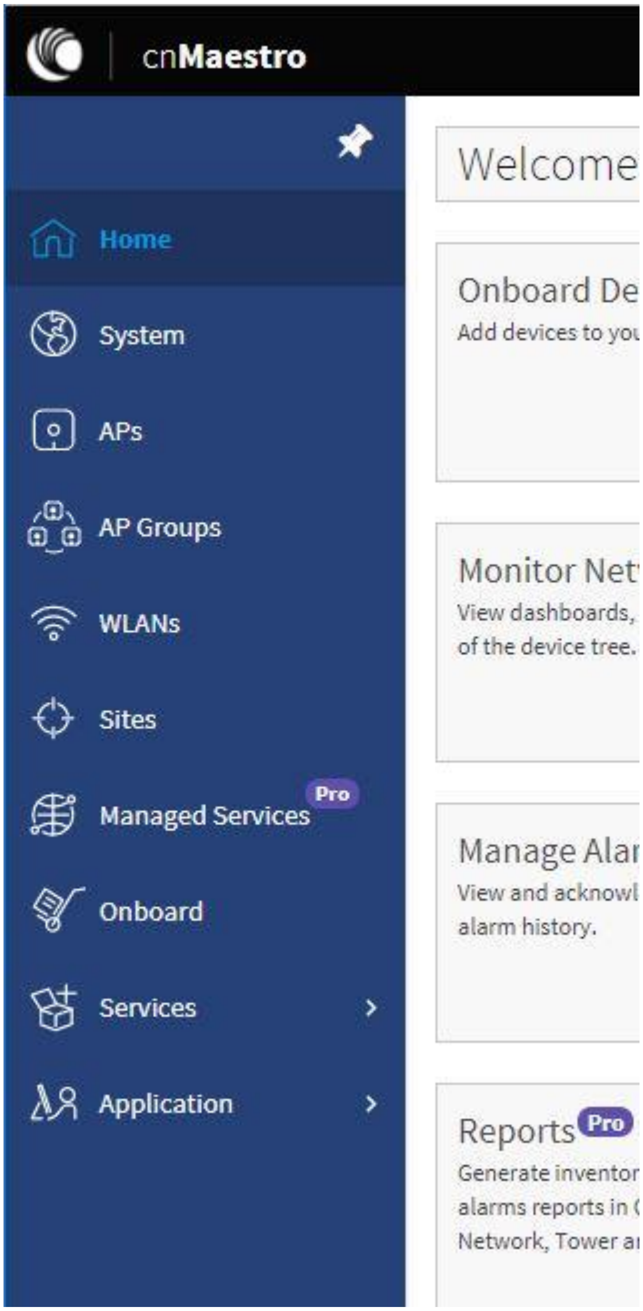
Reports Pro
Generate inventory, performance, events and alarm
reports in CSV format available at System, Network,
Tower and Site level.

Managed Services Pro
Delegate infrastructure adminstration to "Managed
Accounts" managers.

Home will get you to where you already are, so it would seem that choosing System next makes the most sense. However, this will only show you that you don't have anything configured yet. In fact, what you will find is that the menu order does make a lot of sense *once you have a network up and running*. For the initial configuration it is easier to start at the bottom.

Expand the Menu

Until you are familiar with all of the menu options in blue on the left, it can be more convenient to click on the symbol of a pushpin at the top to expand this menu to include the titles of each icon.



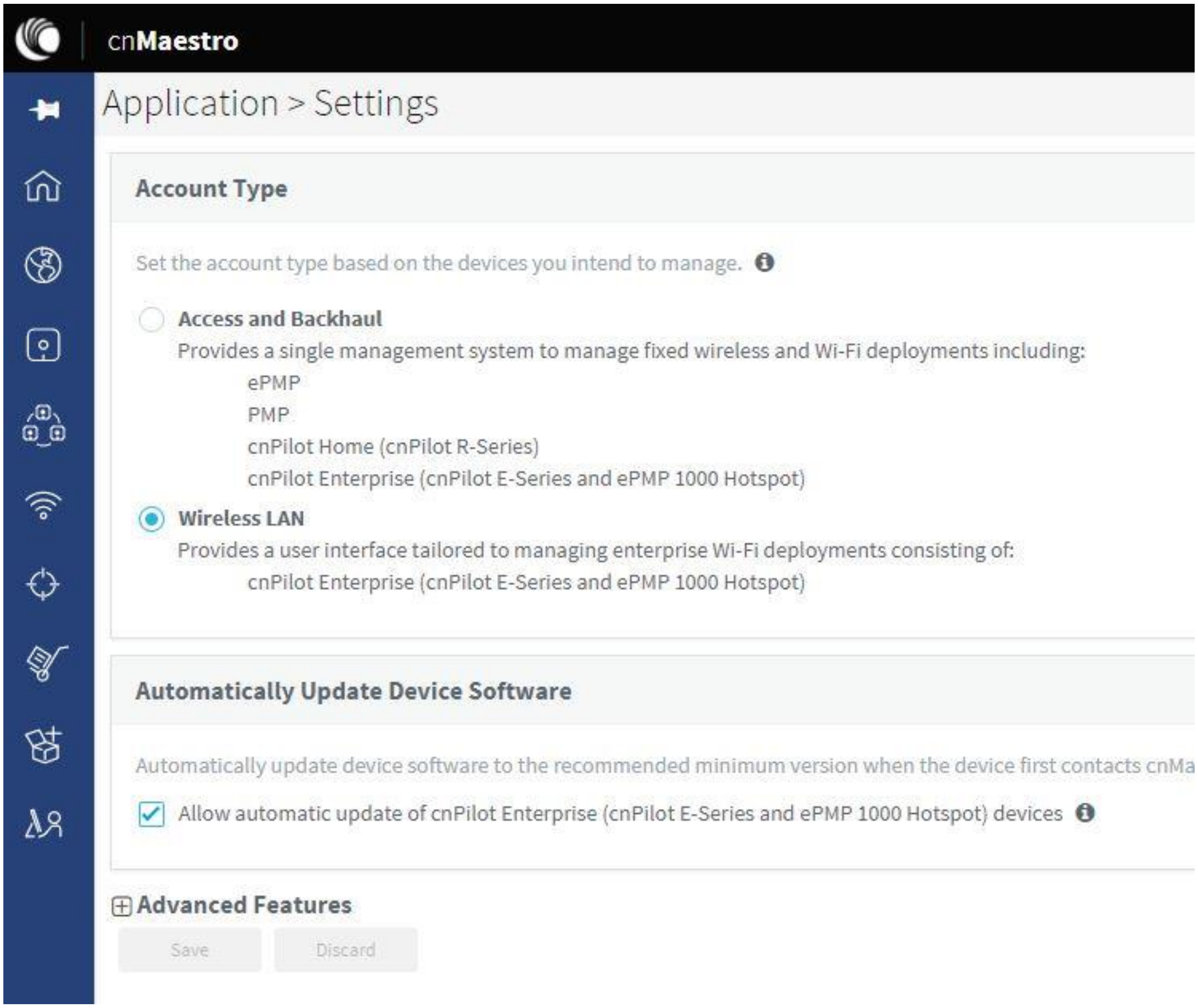
Now you can read the labels for each menu option and even see which ones can be expanded farther. Once you are familiar with these options, clicking on the pushpin again will shrink down the menu to allow more screen space for the information associated with each one.

Application

Instead of starting from the top, we are going to start from the bottom. The bottom option in the blue menu selection is Application. From this menu selection, you can add new users, monitor and affect Jobs (such as software updates), change cnMaestro settings, and enforce configuration synchronization. I will only cover what is needed in most cases to get set up. That is also true for the sections to follow within this document.

Settings

If you are following along with your own cnMaestro account, you may have noticed that the menu options I am showing here do not follow exactly with your own. That is because I have mine set up specifically for a network that does not have any PtMP or R-Series APs being monitored. If you do, you can still do everything that I will cover here, but you will need to navigate slightly differently from time to time. If your network consists of only E-Series (cnPilot) APs being monitored by cnMaestro, you can change the display to look like mine by selecting Settings and then choosing the option optimized for this type of network – Wireless LAN. I also suggest enabling the automatic update of device software when a device is first onboarded.



Application > Settings

Account Type

Set the account type based on the devices you intend to manage.

○ **Access and Backhaul**
Provides a single management system to manage fixed wireless and Wi-Fi deployments including:
ePMP
PMP
cnPilot Home (cnPilot R-Series)
cnPilot Enterprise (cnPilot E-Series and ePMP 1000 Hotspot)

● **Wireless LAN**
Provides a user interface tailored to managing enterprise Wi-Fi deployments consisting of:
cnPilot Enterprise (cnPilot E-Series and ePMP 1000 Hotspot)

Automatically Update Device Software

Automatically update device software to the recommended minimum version when the device first contacts cnMa

☑ Allow automatic update of cnPilot Enterprise (cnPilot E-Series and ePMP 1000 Hotspot) devices

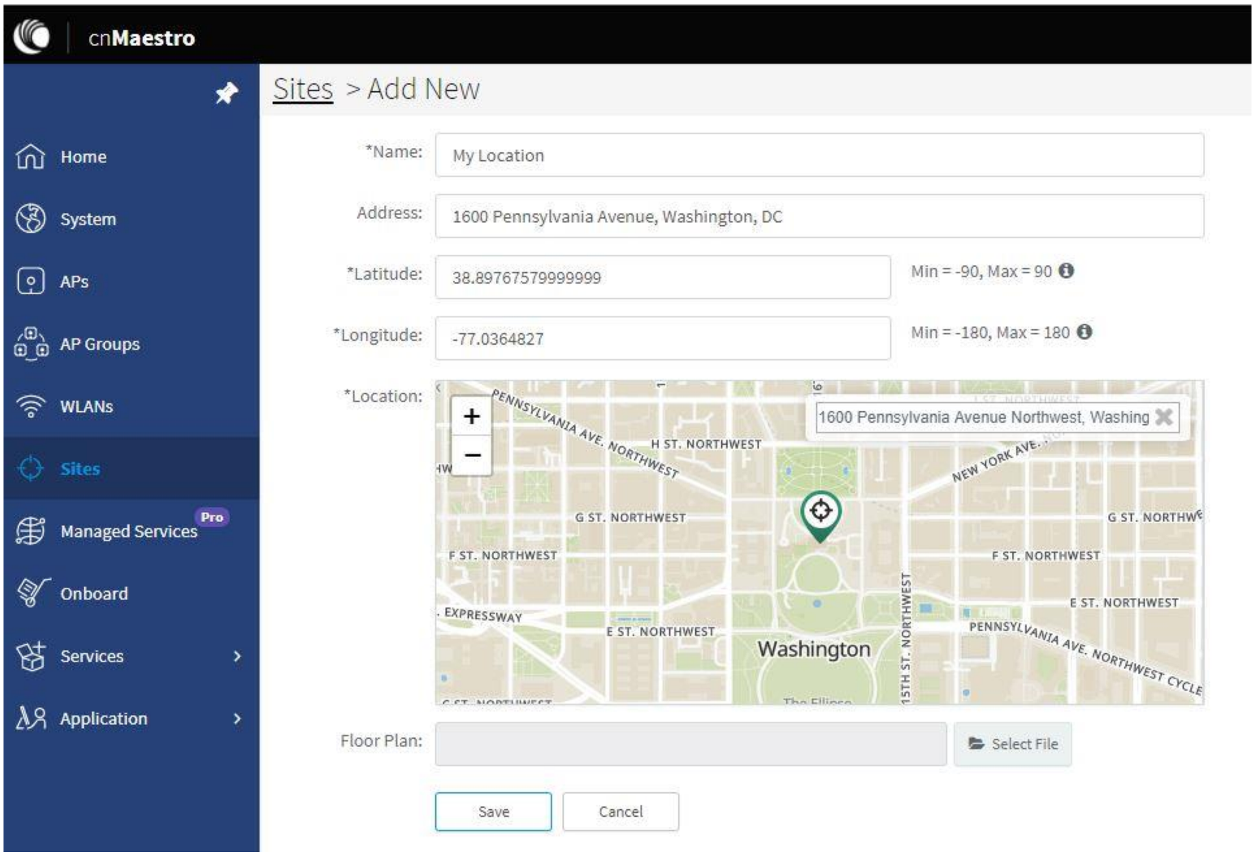
Services

If you are going to setup a Guest WLAN, it is wise to create a Guest Portal before trying to configure a Guest WLAN. You can then assign a Guest Portal to one or more Guest WLANs. We won't cover Guest Portal configurations here. That is covered well in other documentation.

Sites

Moving up the menu, the next stop is Sites. This step is not required, but it is helpful. You can define multiple Sites and indicate where your APs are located by assigning Sites to them. Keep in mind that an AP Group is a group of APs that share the same base configuration. If you make a change to an AP Group, that change is applied to all APs within the group. However, different APs within an AP Group can be located at different Sites. Each Site could have APs from multiple AP Groups. Each AP Group could be located across multiple Sites. Making a change to a Site will only change the Site information. Sites are used for organizing information.

When you Select Sites, you have the option to view previously created sites and to create a new one. Select New Site next. From here you can enter information about the site. If you type in the address in the map window, the GPS coordinates will automatically fill in. From there you can move the location icon to get an even more accurate GPS location.



Sites > Add New

*Name: My Location

Address: 1600 Pennsylvania Avenue, Washington, DC

*Latitude: 38.89767579999999 Min = -90, Max = 90

*Longitude: -77.0364827 Min = -180, Max = 180

*Location: 1600 Pennsylvania Avenue Northwest, Washing

Floor Plan: Select File

You can also add a Floorplan for the site and place APs assigned to this Site in their correct location within the Floorplan. As we have not added any APs yet, though, we will skip this step for now. It should also be pointed out, at the time this document was written, only one Floorplan per Site can be added. This means that if you have a multi-floor building and want to include floorplans for each story, you will want to create a new site per floor. The ability to add multiple floorplans per site is a feature that is planned for a future version of cnMaestro.

Be sure to save your changes.

WLANs

Moving up a bit more, the next step is to add the WLANs that you will be using. You can always add more later, but you will need at least one WLAN created in order to complete a base configuration. Each WLAN can be assigned to more or more AP Groups.

Click on WLANs and then select New WLAN. From here you will see the configuration options for a WLAN to include the basic configuration settings, AAA Servers, Guest Access, Access Control, and Passpoint. For the purposes of this document I will limit the discussion to the basic configuration and one point about Guest Access.

Basic WLAN Configuration

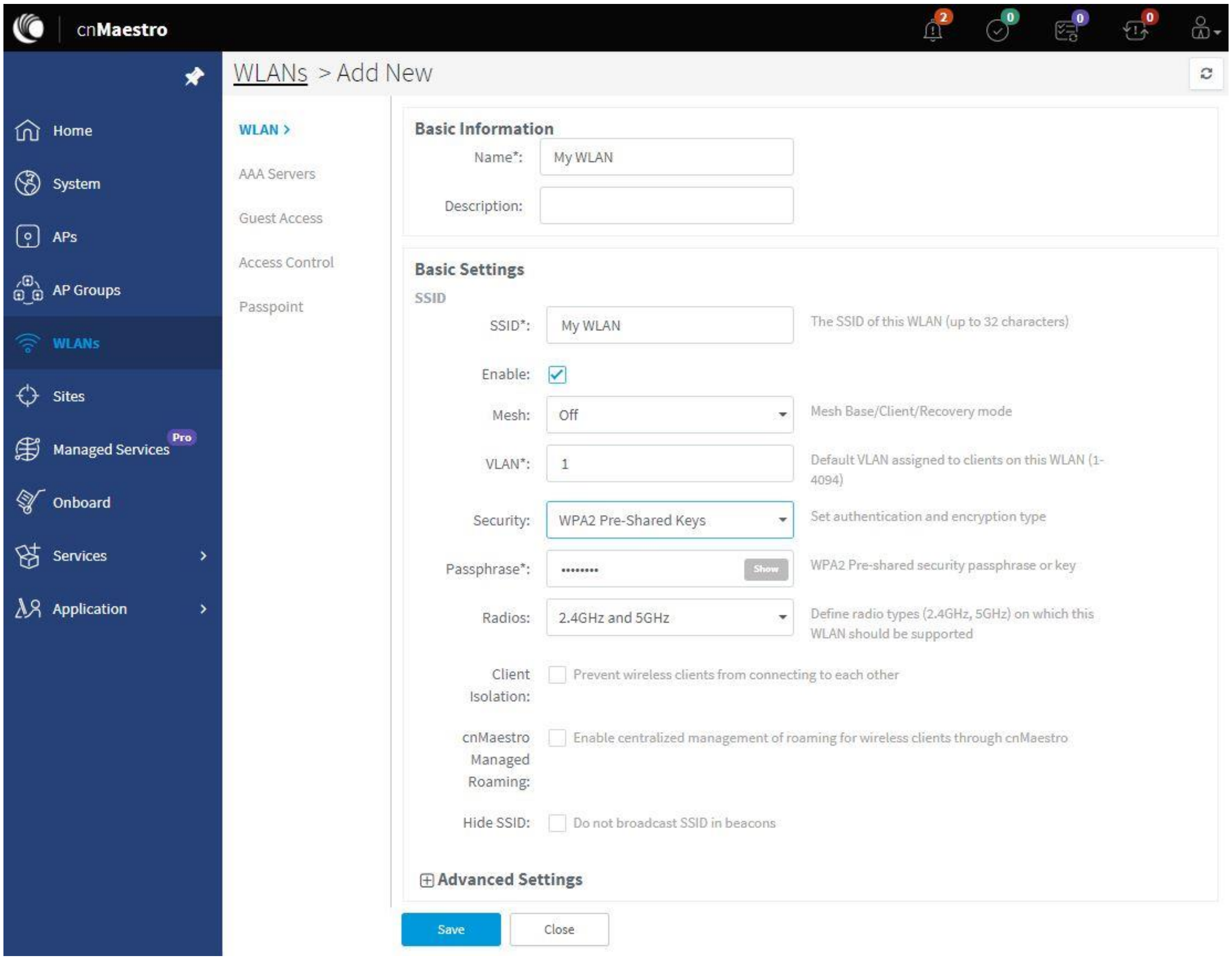
After clicking on WLANs in the blue menu on the left, make certain that "WLAN" is selected in the menu options just to the right of that. You will note that some options have an asterisk next to them. This indicates that information must be entered into those fields in order to be saved. These field include a Name, the SSID, and the VLAN.

The Name and SSID are commonly the same, although this is not strictly necessary. When you fill in the Name, the SSID will automatically fill in with the same value. This can be changed if desired. By default, the VLAN is set to 1. And by default VLAN 1 is set to be untagged. You can only assign a VLAN to a WLAN in this menu; you cannot change the VLAN characteristics (such as whether or not it is tagged) until you move to the AP Group menu options.

At this point, you can choose to leave the WLAN enabled or disable it. Disabling it allows you to send all of the configuration to your APs now, but not have the SSID broadcast until you later decide to do so.

Other options that are typically chose here are the Security setting (Open, WPA2-PSK, and WPA2-Enterprise being the most common), over which radios the WLAN will be used, and whether or not to enforce Client Isolation. Client Isolation prevents WiFi clients from communicating with each over and is a good option if this WLAN is used for Guest access.

Choose your options and be sure to save them.



WLANs > Add New

Basic Information

Name*: My WLAN

Description:

Basic Settings

SSID

SSID*: My WLAN — The SSID of this WLAN (up to 32 characters)

Enable: ☑

Mesh: Off — Mesh Base/Client/Recovery mode

VLAN*: 1 — Default VLAN assigned to clients on this WLAN (1-4094)

Security: WPA2 Pre-Shared Keys — Set authentication and encryption type

Passphrase*: •••••••• — WPA2 Pre-shared security passphrase or key

Radios: 2.4GHz and 5GHz — Define radio types (2.4GHz, 5GHz) on which this WLAN should be supported

Client Isolation: □ Prevent wireless clients from connecting to each other

cnMaestro Managed Roaming: □ Enable centralized management of roaming for wireless clients through cnMaestro

Hide SSID: □ Do not broadcast SSID in beacons

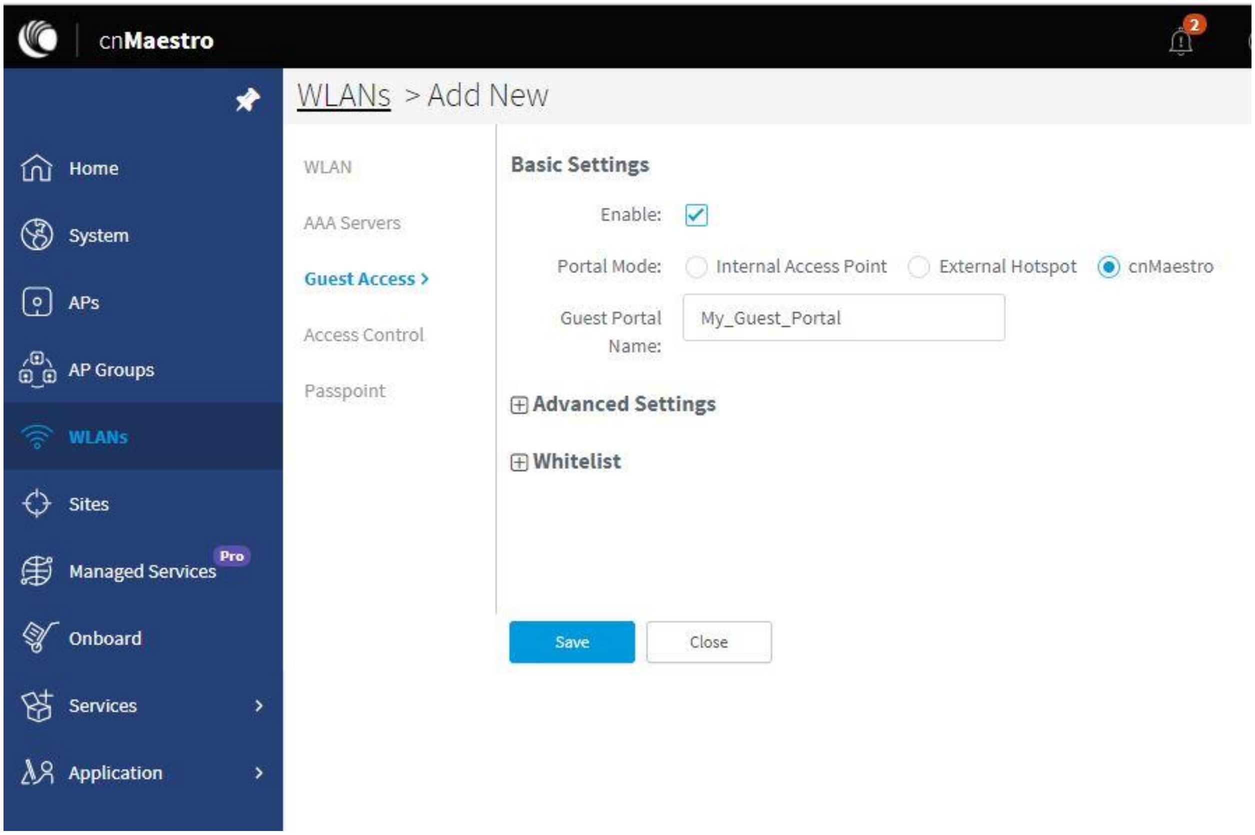
⊞ Advanced Settings

Guest Access

Although this document will not cover the fine details of setting up a Guest WLAN, I will cover some basics here. Select the Guest Access menu option. From here, if you choose to make this new WLAN a Guest WLAN, first enable Guest Access at the top of the configuration options list.

Next, you will see three options for the Guest Portal.

- Internal Access Point. Each AP has the ability to operate a separate Guest Portal instance. This is the least used option as it is more common for the Guest WLAN to appear on more than one AP. In this case, one of the other two options will server client much more efficiently, allowing roaming between APs.
- External Hotspot. With this option, you can direct clients through an external hotspot service when connecting to this WLAN.
- cnMaestro. With this option, you can utilize the Guest Portal that is created under Services and referenced earlier. This is the most commonly used option. When you utilize this option, you will need to fill in the name of the Guest Portal service created earlier *exactly as it was named when created*. This is why I suggested creating the portal before creating the WLAN.



Basic Settings

Enable: ☑

Portal Mode: ○ Internal Access Point ○ External Hotspot ● cnMaestro

Guest Portal Name: My_Guest_Portal

⊞ Advanced Settings

⊞ Whitelist

AP Groups

Next, we move up the list in the blue menu options and select AP Groups. This is where the bulk of the configuration occurs. From here you will select the WLANs to be assigned to APs and configure Management, Radio, Network, Tunneling, and other settings. We will only cover the most common used options here.

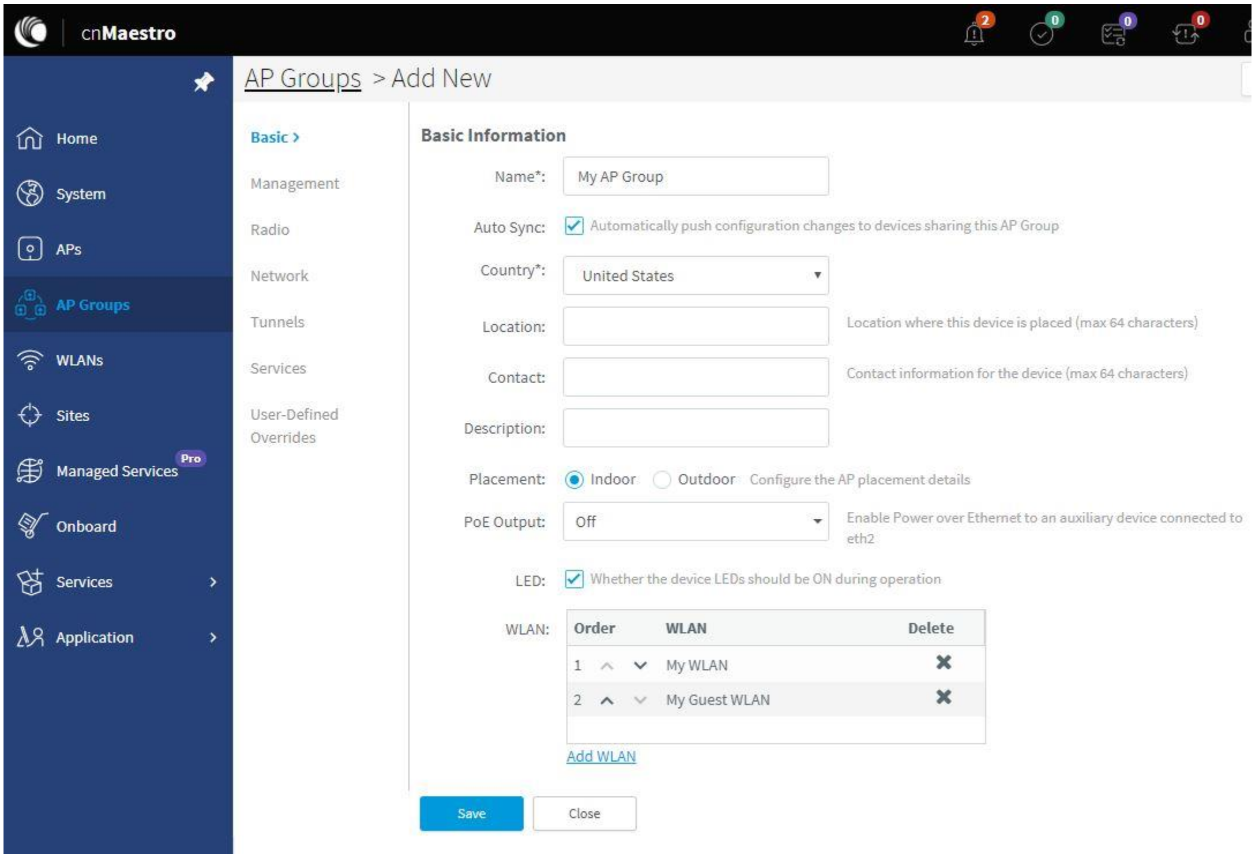
Basic

After clicking on AP Groups, select Add New AP Group and begin configuring the Basic settings for your new AP Group. Again, you will see a couple fields that are mandatory as indicated by an asterisk. You must have a name for your AP Group and a Country. The Country field will assign the Country Code settings to the APs. If you are deploying in a country such as the US where the regulatory agencies dictate that a country code must be locked down in the AP before it is shipped, you will need to choose the right option before cnMaesto can even affect any other configuration changes to your APs. In many countries around the world, you can actually change the country code on the AP by changing this setting in cnMaestro. In the US, Israel, and Japan that is locked down in the AP and must match what is set in cnMaestro.

Depending on your country code settings, choosing Indoor or Outdoor placement will affect what EIRP limitations are adhered to as regulations can vary between indoor and outdoor deployments. In the US this is no longer the case, so this option does not affect your APs.

You must also choose as least one WLAN from those that you created earlier. Click on Add WLAN to see a list of WLANs from those that you have already created. Again, this is why I suggested creating the WLANs before creating the AP Group.

Make your selections and be sure to save.



Basic Information

Name*: My AP Group

Auto Sync: ☑ Automatically push configuration changes to devices sharing this AP Group

Country*: United States

Location: Location where this device is placed (max 64 characters)

Contact: Contact information for the device (max 64 characters)

Description:

Placement: ● Indoor ○ Outdoor Configure the AP placement details

PoE Output: Off Enable Power over Ethernet to an auxiliary device connected to eth2

LED: ☑ Whether the device LEDs should be ON during operation

WLAN:

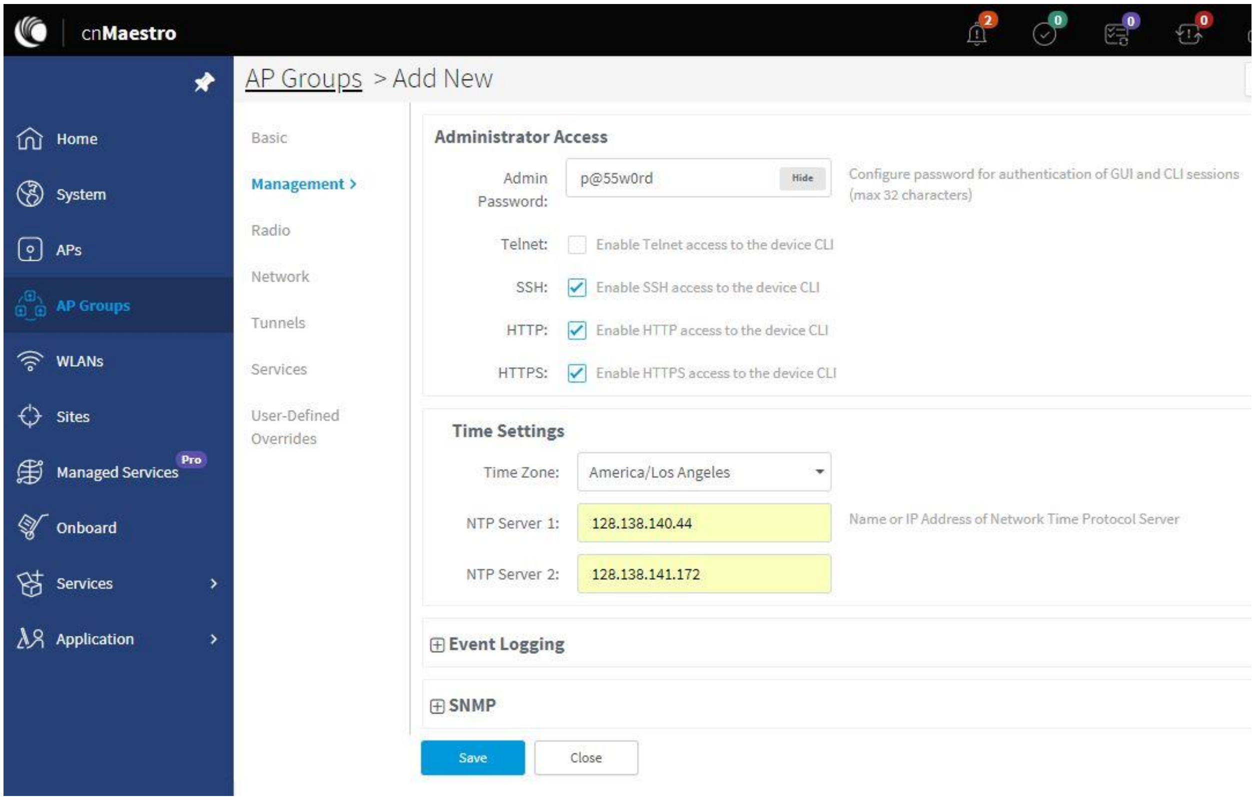
Order	WLAN	Delete
1	My WLAN	✖
2	My Guest WLAN	✖

Add WLAN

Management

Next select Management. From here you will want to change the default password, which is “Admin”. You can also specify the methods through which management access can occur on the APs based on your organizations security standards.

Setting the Time Zone and specifying NTP servers will give your logs more meaning. Although not a requirement, I do recommend completing this step.



AP Groups > Add New

Administrator Access

Admin Password: p@55w0rd — Configure password for authentication of GUI and CLI sessions (max 32 characters)

Telnet: ☐ Enable Telnet access to the device CLI

SSH: ☑ Enable SSH access to the device CLI

HTTP: ☑ Enable HTTP access to the device CLI

HTTPS: ☑ Enable HTTPS access to the device CLI

Time Settings

Time Zone: America/Los Angeles

NTP Server 1: 128.138.140.44 — Name or IP Address of Network Time Protocol Server

NTP Server 2: 128.138.141.172

⊞ Event Logging

⊞ SNMP

Be sure to save your changes.

Radio

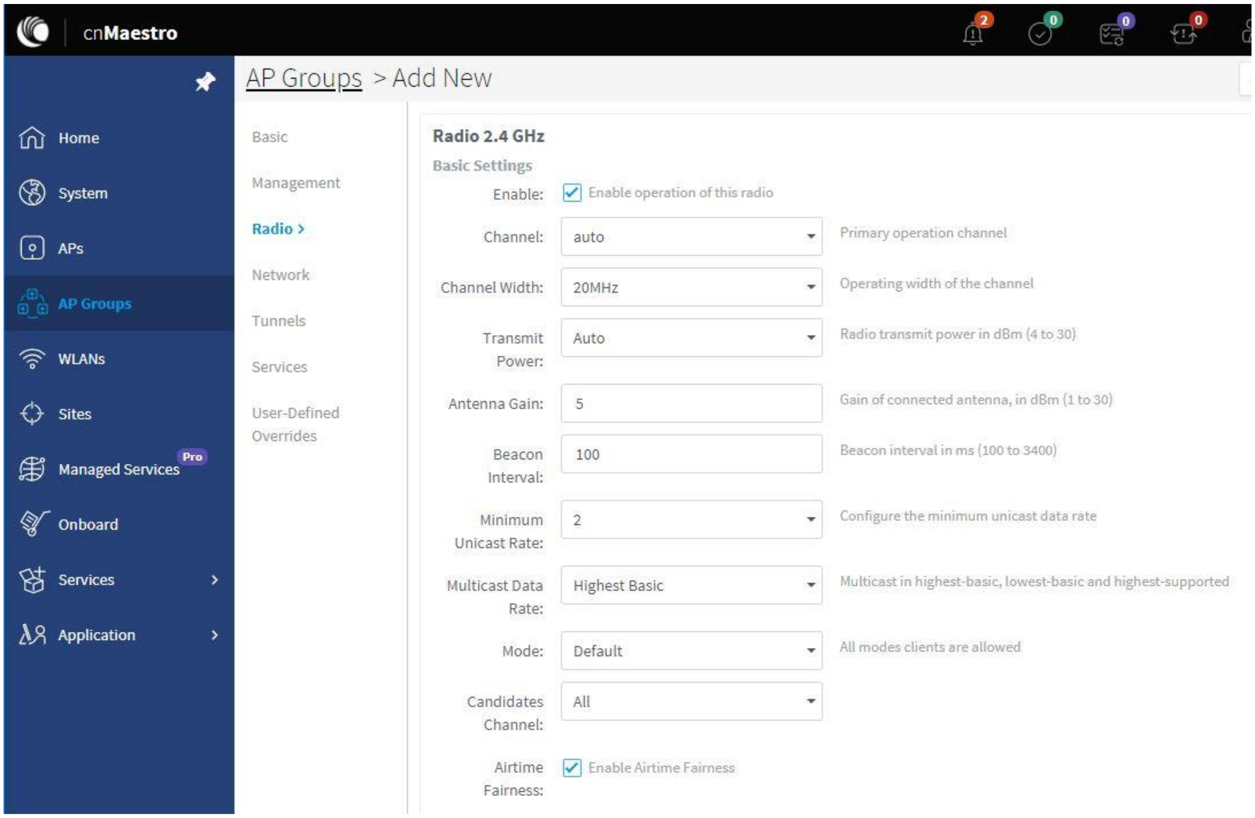
Next, select Radio. From here you will make changes to channel settings, transmit power, and affect both roaming and interference mitigation capabilities. This is where the more meaty changes will occur from the default settings. I highly recommend following the options that I have selected below for the vast majority of deployment types.

2.4 GHz

Each radio in the AP is configured separately. Be certain to complete configuration changes for both the 2.4 GHz and 5 GHz radios. The menu starts with 2.4 GHz, so we will too.

- Enable. From here you can choose to enable or disable the 2.4 GHz radio. There are times, especially in very high density deployment, when you may choose to disable some of the 2.4 GHz radios, using only 5 GHz. For this, you will want to create two different AP Groups. One with 2.4 GHz enabled and one with 2.4 GHz disabled.

- Channel. I recommend leaving this at the default setting of auto, allowing the APs to choose their own channels based on RF conditions.
- Channel Width. I recommend using 20 MHz. It is possible to use 40 MHz, but it is rare that the 2.4 GHz environment will make this a wise choice.
- Transmit Power. I recommend leaving this as Auto as well. We will make other configuration changes later that will allow the APs to best choose when to turn down power and when to turn it up.
- Antenna Gain. This field is not relevant for APs with internal, fixed antennas. This is the case for all cnPilot models today. Leave this field as it is.
- Beacon Interval, Multicast Data Rate, Mode, and Candidates Channel. For the majority of deployments, I suggest leaving these settings at default.
- Minimum Unicast Rate. Changing this value will tell the AP to advertise to all clients that it will only accept clients that can connect at this minimum MCS rate. When left at the default of 1, clients will attempt to connect at the far reach of the AP, even when conditions are poor enough that connections are not guaranteed. To make this worse, some clients tend to stay connected to an AP when they should roam to another one. By raising this value, you will shrink the cell size of each AP, but you will also do so in a manner that both ensures more solid connections between AP and client and will encourage clients to roam more quickly. At a minimum, I suggest raising this value to 2. If you want to exclude all 802.11b clients, raise this value to 12.
- Airtime Fairness. Enable Airtime Fairness in order to prevent slower 802.11b and g clients from forcing the faster 802.11n clients down to their speed.



AP Groups > Add New

Radio 2.4 GHz

Basic Settings

Enable: ☑ Enable operation of this radio

Channel: auto — Primary operation channel

Channel Width: 20MHz — Operating width of the channel

Transmit Power: Auto — Radio transmit power in dBm (4 to 30)

Antenna Gain: 5 — Gain of connected antenna, in dBm (1 to 30)

Beacon Interval: 100 — Beacon interval in ms (100 to 3400)

Minimum Unicast Rate: 2 — Configure the minimum unicast data rate

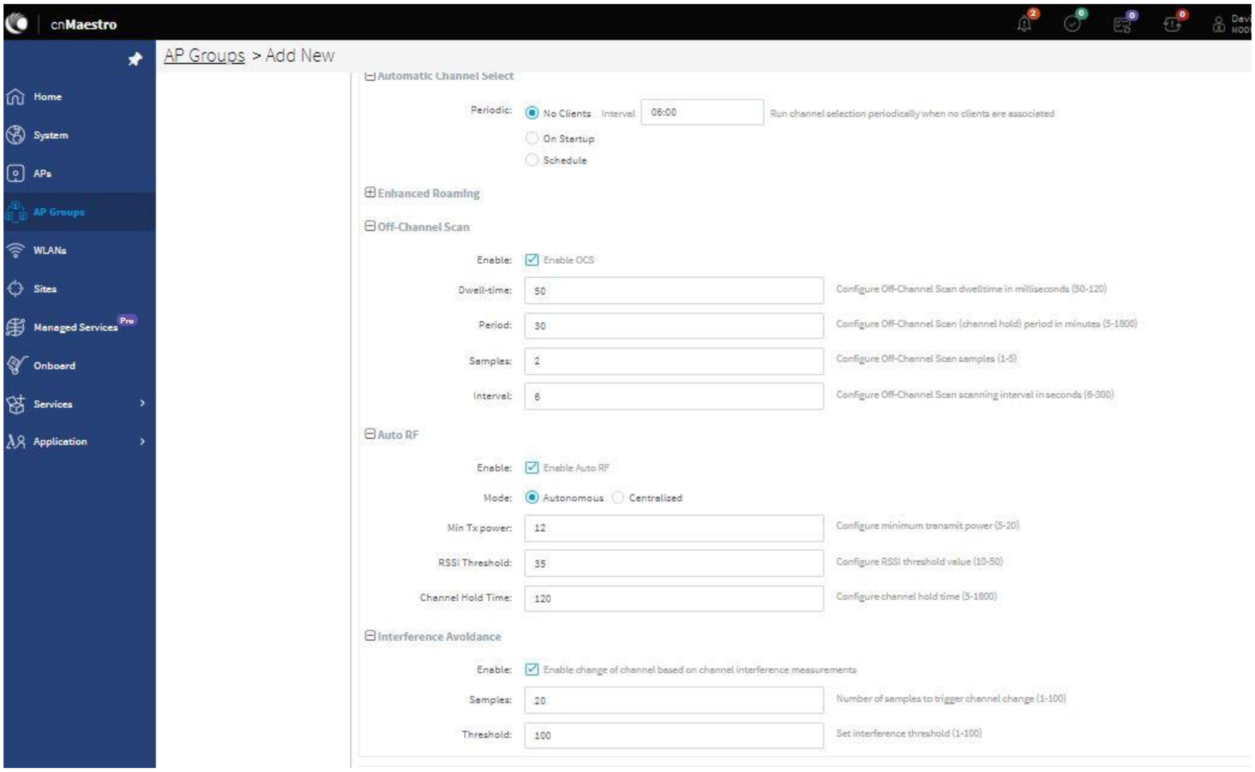
Multicast Data Rate: Highest Basic — Multicast in highest-basic, lowest-basic and highest-supported

Mode: Default — All modes clients are allowed

Candidates Channel: All

Airtime Fairness: ☑ Enable Airtime Fairness

- Automatic Channel Select. Enable this feature and choose “No Clients” with the default interval of 6 minutes. This will allow the APs to choose the best channel possible whenever there are no clients connected to them every 6 minutes.
- Enhanced Roaming. Do not enable this feature. It is a nice feature to have if you have very sticky clients, ones that absolutely refuse to roam. But it is a harsh approach that can better be served for most clients by adjusting the Minimum Unicast Rate as mentioned earlier. Fortunately, very sticky clients are quite rare today.
- Off Channel Scan. Enable this feature and use the default settings. This will tell the APs to go offline very briefly to scan other channels in order to build up a reference table of which channels they can use if a channel change becomes necessary. This will not drop clients.
- Auto RF. Enable this feature using the default settings. This will tell APs to turn down their power if they are in close proximity to another AP that you own running on the same channel with enough power to cause interference. If that changes later, because one of them fails or their channel changes, the AP will then increase power again.
- Interference Avoidance. Enable this feature using the default settings. Enabling this feature will allow the AP to change channels if certain thresholds are exceeded. When this occurs, the AP will send out an 802.11h message telling all clients that it is about to change channels and to what channel so they will be able to follow.



⊟ Automatic Channel Select

Periodic: ● No Clients Interval 06:00 Run channel selection periodically when no clients are associated
○ On Startup
○ Schedule

⊞ Enhanced Roaming

⊟ Off-Channel Scan

Enable: ☑ Enable OCS
Dwell-time: 50 Configure Off-Channel Scan dwelltime in milliseconds (50-120)
Period: 30 Configure Off-Channel Scan (channel hold) period in minutes (5-1800)
Samples: 2 Configure Off-Channel Scan samples (1-5)
Interval: 6 Configure Off-Channel Scan scanning interval in seconds (6-300)

⊟ Auto RF

Enable: ☑ Enable Auto RF
Mode: ● Autonomous ○ Centralized
Min Tx power: 12 Configure minimum transmit power (5-20)
RSSI Threshold: 35 Configure RSSI threshold value (10-50)
Channel Hold Time: 120 Configure channel hold time (5-1800)

⊟ Interference Avoidance

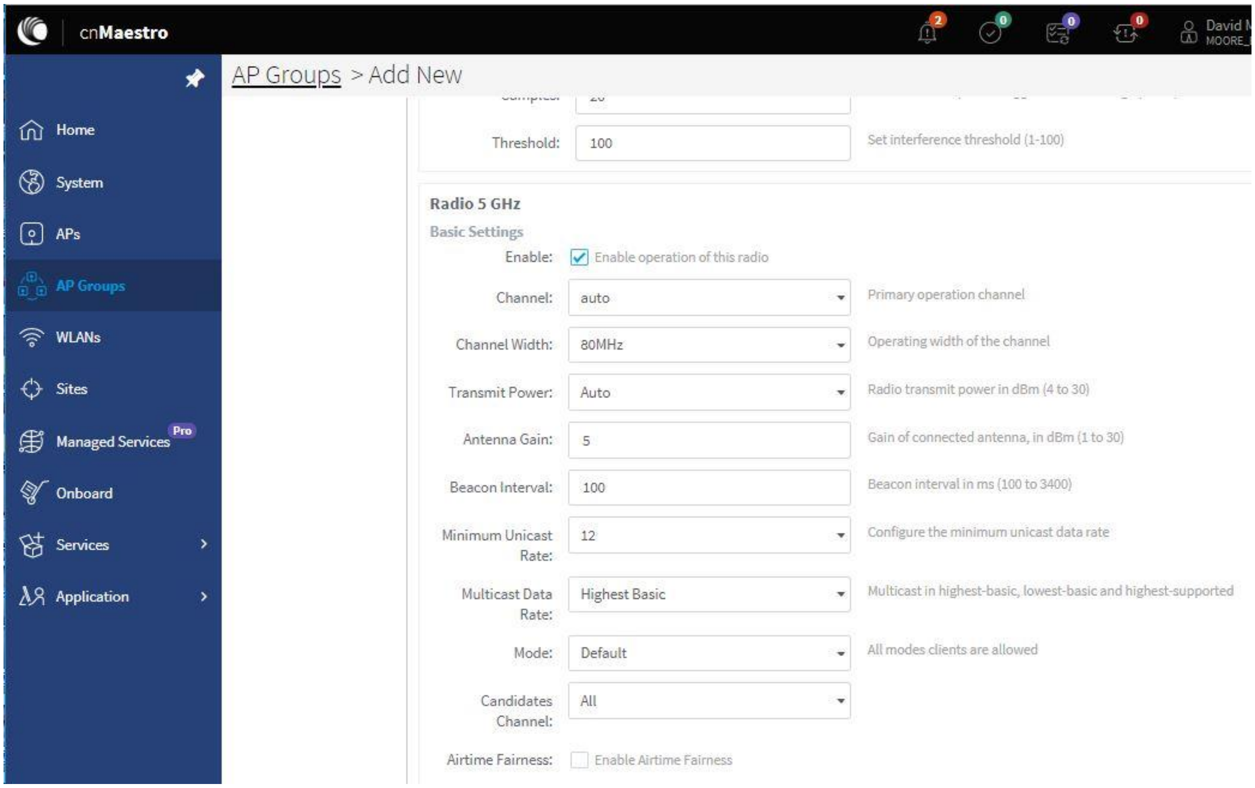
Enable: ☑ Enable change of channel based on channel interference measurements
Samples: 20 Number of samples to trigger channel change (1-100)
Threshold: 100 Set interference threshold (1-100)

5 GHz

Except where there are differences with the 2.4 GHz radio settings, I will not expound on the reasoning behind the recommended settings for 5 GHz below.

- Channel, Transmit Power, Antenna Gain, Beacon Interval, Multicast Data Rate, and Mode. Leave at the default settings.

- Channel Width. The default is 80 MHz. I strongly recommend changing this at least to 40 MHz, with 20 MHz being the best choice in most circumstances. Finding a clear channel that is smaller is much more simple than when they are wide. If you deploy multiple APs, you will want them to be as separated in the spectrum as they can be to maximize capacity and throughput (really, the same thing). 20 MHz channels will do this and will generally provide the best overall throughput.
- Minimum Unicast Rate. Changing this is less important than it is for 2.4 GHz as the long tail of coverage seen with a 1 Mb/s rate on 2.4 GHz is much more pronounced than 6 Mb/s is on 5 GHz. However, I often find that using 12 Mb/s on 5 GHz yields the best roaming results. For good roaming, you will also want to design for good overlap of coverage at this data rate.
- Candidates Channel. In most cases, leaving this at default of All is the best choice. However, if you have clients that do not support DFS channels, you can select non-DFS preferred. Or, if you are deploying outdoors and want to reserve some 5 GHz channels for PtMP radios and others for WiFi APs, you can set the list of channels from which the AP's can choose here.
- Airtime Fairness. I am ambivalent about Airtime Fairness in 5 GHz. Previous to the prevalence of 802.11ac clients in 5 GHz, this feature did offer good separation of client speeds, preventing the slower 802.11a clients from forcing 802.11n clients to their speed. 802.11ac, however, has measures built in, like better block acknowledgment, to prevent this from being an issue. And, it is possible for Airtime Fairness to actually slow down 802.11ac clients. My recommendation is to leave it disabled.



AP Groups > Add New

Threshold: 100 — Set interference threshold (1-100)

Radio 5 GHz

Basic Settings

Enable: ☑ Enable operation of this radio

Channel: auto — Primary operation channel

Channel Width: 80MHz — Operating width of the channel

Transmit Power: Auto — Radio transmit power in dBm (4 to 30)

Antenna Gain: 5 — Gain of connected antenna, in dBm (1 to 30)

Beacon Interval: 100 — Beacon interval in ms (100 to 3400)

Minimum Unicast Rate: 12 — Configure the minimum unicast data rate

Multicast Data Rate: Highest Basic — Multicast in highest-basic, lowest-basic and highest-supported

Mode: Default — All modes clients are allowed

Candidates Channel: All

Airtime Fairness: ☐ Enable Airtime Fairness

- Automatic Channel Select. Enable, choosing "No Clients" and the default of 6 minutes.

- Enhanced Roaming. Do not enable.
- Off-Channel Scan. Enable, using the default settings.
- Auto RF. Enable, using the default settings.
- Interference Avoidance. Enable, using the default settings.

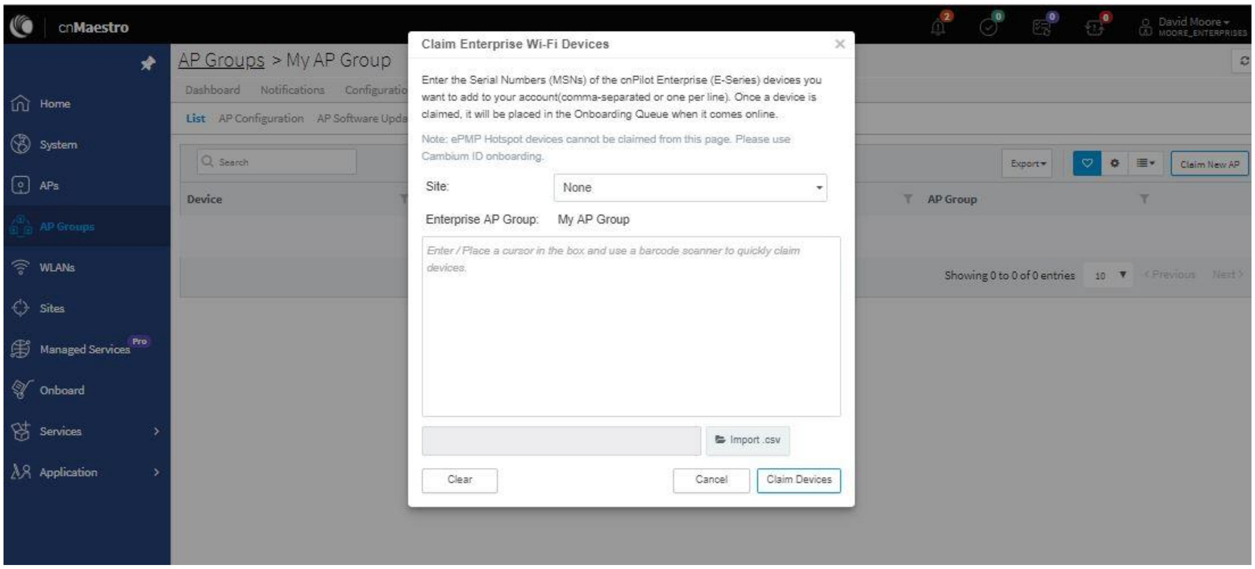
Be sure to save your changes.

Onboarding APs to your new AP Group

The next step is to onboard your new APs. If you have already done this, you don't need to do this step, but you will want to assign each AP to an AP Group. In most cases, that will mean that they will all be in the same AP Group. If you started fresh and did the steps in the order I have outlined, then you can import your APs now, assign them to a Site, and assign them to an AP Group all in one step.

Click on AP Groups in the blue menu on the left. Even though you were already editing your AP Group before, this will bring you back to the main AP Group menu where you will see your newly created AP Group along with the Default Enterprise AP Group that we provide as an example. Click on the name of your AP Group and you will be brought to the dashboard for that AP Group. It won't be very interesting initially as there are no APs assigned to it, no clients, and no traffic. But we will solve that now.

Click on the menu option in the grey bar near the top that reads "APs". At this point, there will be no APs listed, but you will see a button to Claim a New AP on the right hand side. Click on this button.



Claim Enterprise Wi-Fi Devices

Enter the Serial Numbers (MSNs) of the cnPilot Enterprise (E-Series) devices you want to add to your account(comma-separated or one per line). Once a device is claimed, it will be placed in the Onboarding Queue when it comes online.

Note: ePMP Hotspot devices cannot be claimed from this page. Please use Cambium ID onboarding.

Site: None

Enterprise AP Group: My AP Group

Enter / Place a cursor in the box and use a barcode scanner to quickly claim devices.

What you will see will look like what is shown above. The first thing you should note is that you have a drop-down box to select one of the Sites that you created. You do not need to assign a Site here, but if all of your APs in your AP Group are located at one Site, it is convenient to set that now.

Next, type in the MSN for each of your APs in the box. You can separate these line by line or just with a comma. You can also use a bar code scanning to scan the bar code on either the box or the AP itself for the MSNs. Save this list to a CSV file and then import it using the "Import .CSV" button. Once you have typed and/or imported your list, click on Claim Devices. You can follow the progress as they contact the public cloud and come online.

Hint. If you are impatient like me. Either do not plug in your APs until you have already entered their MSNs and clicked on Claim Devices or reboot the APs right after you do. As soon as the APs finish booting up they will reach out to cnMaestro. But if they have been plugged in a while, they will only reach out to the server every few minutes. If you are caught in the middle of this cycle, rebooting will ensure that it happens right away.

Configuring through the AP GUI

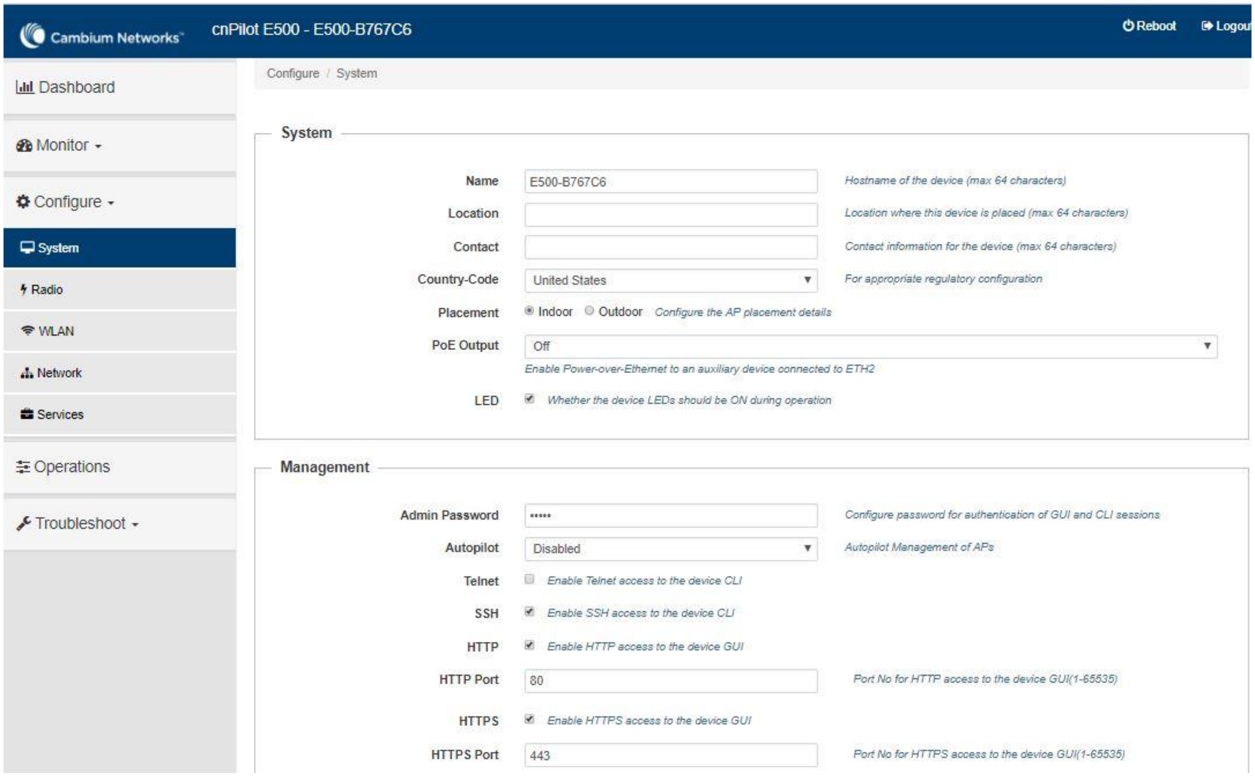
Configuring through cnMaestro is the preferred method. But if you choose, you can also use the AP GUI itself. I would not recommend using this method if you are configuring more than one AP in the same way, or if you plan to use cnMaestro to monitor the APs. In the former case, doing so will mean repeating the same configuration steps multiple times rather than once and applying to all. In the latter case, if you tell cnMaestro to sync configuration, it will overwrite what was done through the AP GUI with what is configured through cnMaestro.

Log into AP GUI

First log into your AP through the web GUI. By default, http is enabled as an access method, so simply typing in the IP address of your AP into your browser will bring up the login screen. The trick is learning the IP address. You may need to check into the DHCP server to find what address is assigned to the AP as DHCP is the default option for obtaining an address. Or, if you do not provide DHCP, you can use the default IP address of 192.168.0.1. In either case, the default login is “admin” and the default password is also “admin”.

Configure System Settings

Next, click on Configure in the left hand menu to expand the options and select System. From here you will set the name, Country Code, Password, Management access options, and Time Settings. The Country-Code cannot be changed for APs sold into the US as the FCC requires that it be locked down. In other locations, you have the ability to set the Country-Code as is appropriate.



System

Name: E500-B767C6 — *Hostname of the device (max 64 characters)*

Location: — *Location where this device is placed (max 64 characters)*

Contact: — *Contact information for the device (max 64 characters)*

Country-Code: United States ▾ — *For appropriate regulatory configuration*

Placement: ● Indoor ○ Outdoor — *Configure the AP placement details*

PoE Output: Off ▾ — *Enable Power-over-Ethernet to an auxiliary device connected to ETH2*

LED: ☑ *Whether the device LEDs should be ON during operation*

Management

Admin Password: ••••• — *Configure password for authentication of GUI and CLI sessions*

Autopilot: Disabled ▾ — *Autopilot Management of APs*

Telnet: ☐ *Enable Telnet access to the device CLI*

SSH: ☑ *Enable SSH access to the device CLI*

HTTP: ☑ *Enable HTTP access to the device GUI*

HTTP Port: 80 — *Port No for HTTP access to the device GUI(1-65535)*

HTTPS: ☑ *Enable HTTPS access to the device GUI*

HTTPS Port: 443 — *Port No for HTTPS access to the device GUI(1-65535)*

Be sure to save your changes.

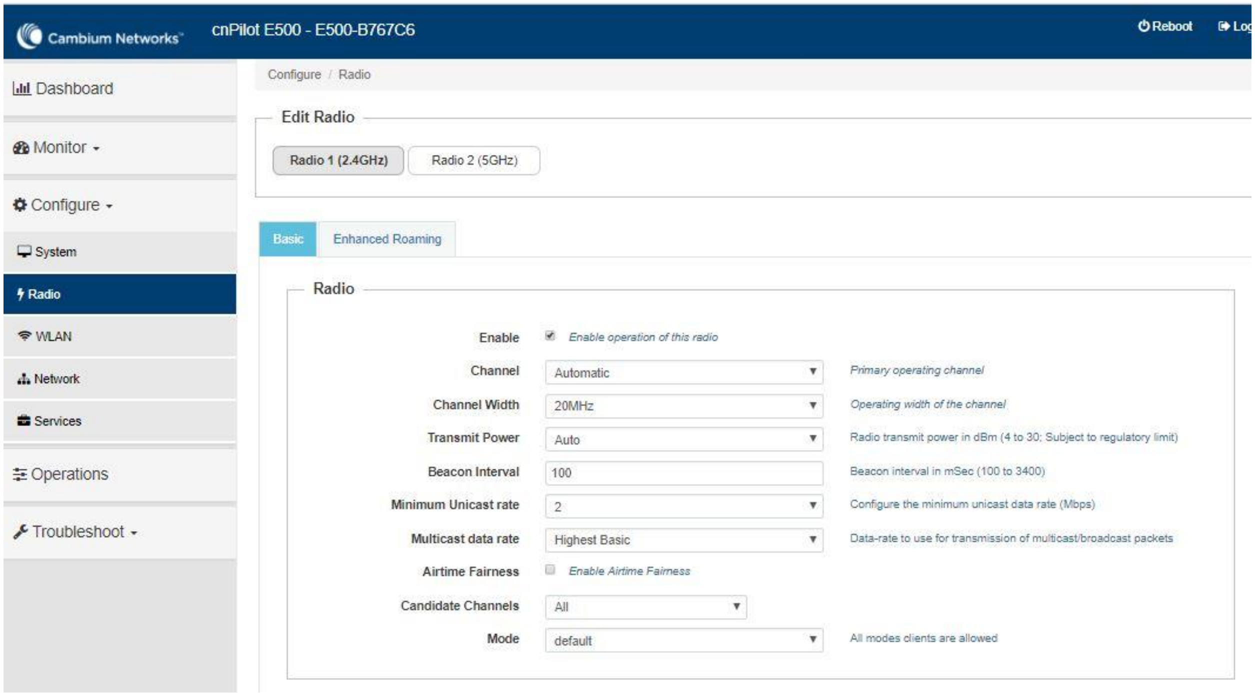
Configure Radio Settings

Next Click on Radio under the Configuration options. You will see that there are buttons for selecting both Radio 1 (2.4 GHz) and Radio 2 (5 GHz). This allows you to configure different settings for each band.

2.4 GHz

- Enable. From here you can choose to enable or disable the 2.4 GHz radio. There are times, especially in very high density deployment, when you may choose to disable some of the 2.4 GHz radios, using only 5 GHz. For this, you will want to create two different AP Groups. One with 2.4 GHz enabled and one with 2.4 GHz disabled.
- Channel. I recommend leaving this at the default setting of auto, allowing the APs to choose their own channels based on RF conditions.
- Channel Width. I recommend using 20 MHz. It is possible to use 40 MHz, but it is rare that the 2.4 GHz environment will make this a wise choice.
- Transmit Power. I recommend leaving this as Auto as well. We will make other configuration changes later that will allow the APs to best choose when to turn down power and when to turn it up.

- Beacon Interval, Multicast Data Rate, Mode, and Candidates Channel. For the majority of deployments, I suggest leaving these settings at default.
- Minimum Unicast Rate. Changing this value will tell the AP to advertise to all clients that it will only accept clients that can connect at this minimum MCS rate. When left at the default of 1, clients will attempt to connect at the far reach of the AP, even when conditions are poor enough that connections are not guaranteed. To make this worse, some clients tend to stay connected to an AP when they should roam to another one. By raising this value, you will shrink the cell size of each AP, but you will also do so in a manner that both ensures more solid connections between AP and client and will encourage clients to roam more quickly. At a minimum, I suggest raising this value to 2. If you want to exclude all 802.11b clients, raise this value to 12.
- Airtime Fairness. Enable Airtime Fairness in order to prevent slower 802.11b and g clients from forcing the faster 802.11n clients down to their speed.

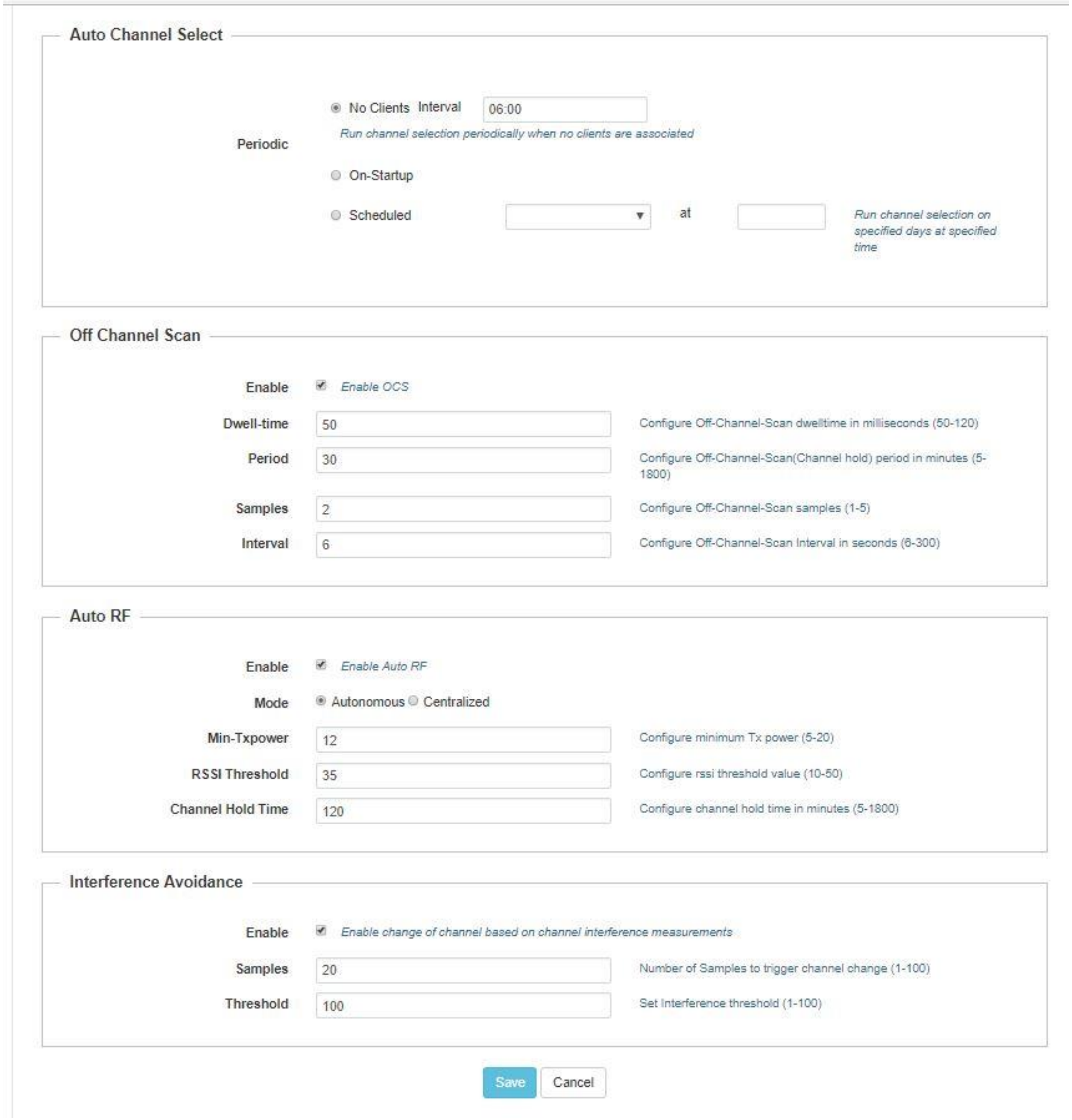


Radio

Enable	☑ Enable operation of this radio	
Channel	Automatic	Primary operating channel
Channel Width	20MHz	Operating width of the channel
Transmit Power	Auto	Radio transmit power in dBm (4 to 30; Subject to regulatory limit)
Beacon Interval	100	Beacon interval in mSec (100 to 3400)
Minimum Unicast rate	2	Configure the minimum unicast data rate (Mbps)
Multicast data rate	Highest Basic	Data-rate to use for transmission of multicast/broadcast packets
Airtime Fairness	☐ Enable Airtime Fairness	
Candidate Channels	All	
Mode	default	All modes clients are allowed

- Automatic Channel Select. Enable this feature and choose “No Clients” with the default interval of 6 minutes. This will allow the APs to choose the best channel possible whenever there are no clients connected to them every 6 minutes.
- Off Channel Scan. Enable this feature and use the default settings. This will tell the APs to go offline very briefly to scan other channels in order to build up a reference table of which channels they can use if a channel change becomes necessary. This will not drop clients.
- Auto RF. Enable this feature using the default settings. This will tell APs to turn down their power if they are in close proximity to another AP that you own running on the same channel with enough power to cause interference. If that changes later, because one of them fails or their channel changes, the AP will then increase power again.
- Interference Avoidance. Enable this feature using the default settings. Enabling this feature will allow the AP to change channels if certain thresholds are exceeded. When this occurs, the AP

will send out an 802.11h message telling all clients that it is about to change channels and to what channel so they will be able to follow.



Auto Channel Select

Periodic
● No Clients Interval 06:00
Run channel selection periodically when no clients are associated
○ On-Startup
○ Scheduled ▾ at *Run channel selection on specified days at specified time*

Off Channel Scan

Enable	☑ *Enable OCS*	
Dwell-time	50	Configure Off-Channel-Scan dwelltime in milliseconds (50-120)
Period	30	Configure Off-Channel-Scan(Channel hold) period in minutes (5-1800)
Samples	2	Configure Off-Channel-Scan samples (1-5)
Interval	6	Configure Off-Channel-Scan Interval in seconds (6-300)

Auto RF

Enable	☑ *Enable Auto RF*	
Mode	● Autonomous ○ Centralized	
Min-Txpower	12	Configure minimum Tx power (5-20)
RSSI Threshold	35	Configure rssi threshold value (10-50)
Channel Hold Time	120	Configure channel hold time in minutes (5-1800)

Interference Avoidance

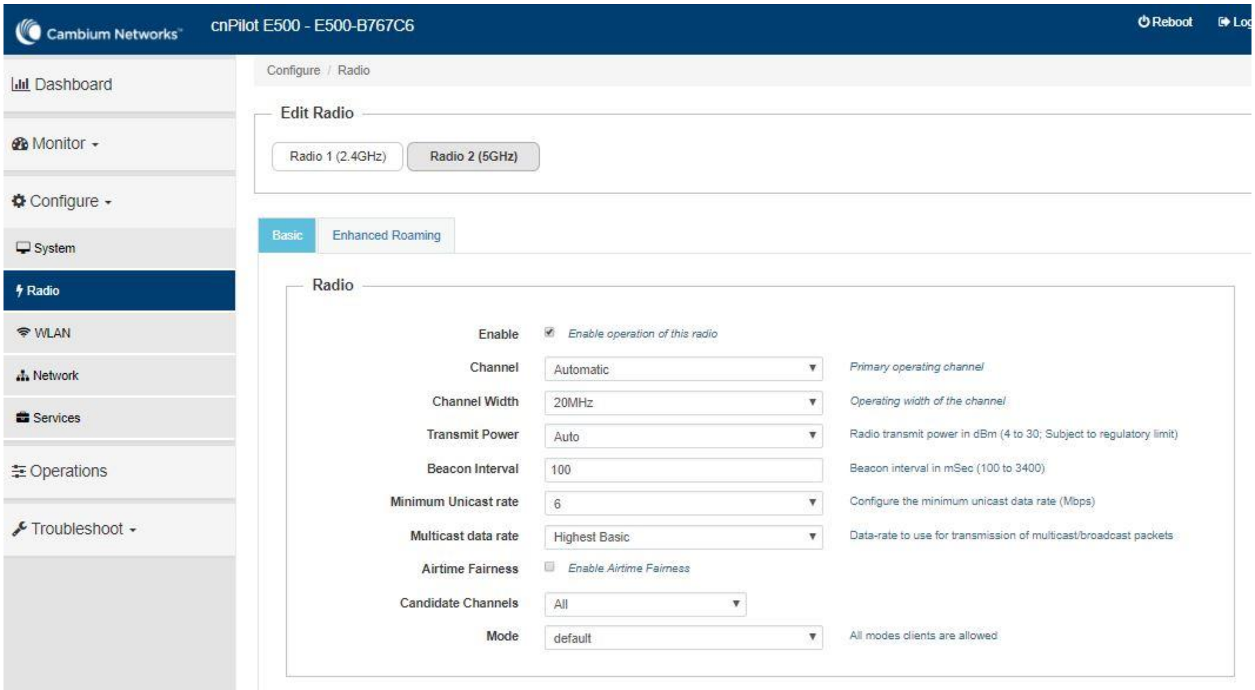
Enable	☑ *Enable change of channel based on channel interference measurements*	
Samples	20	Number of Samples to trigger channel change (1-100)
Threshold	100	Set Interference threshold (1-100)

There is also a tab for Enhanced Roaming. Do not enable Enhanced Roaming. It is a nice feature to have if you have very sticky clients, ones that absolutely refuse to roam. But it is a harsh approach that can better be served for most clients by adjusting the Minimum Unicast Rate as mentioned earlier. Fortunately, very sticky clients are quite rare today.

5 GHz

Next click on the Radio 2 (5 GHz) button at the top in order to configure the 5 GHz radio options. Except where there are differences with the 2.4 GHz radio settings, I will not expound on the reasoning behind the recommended settings for 5 GHz below.

- Channel, Transmit Power, Beacon Interval, Multicast Data Rate, and Mode. Leave at the default settings.
- Channel Width. The default is 80 MHz. I strongly recommend changing this at least to 40 MHz, with 20 MHz being the best choice in most circumstances. Finding a clear channel that is smaller is much more simple than when they are wide. If you deploy multiple APs, you will want them to be as separated in the spectrum as they can be to maximize capacity and throughput (really, the same thing). 20 MHz channels will do this and will generally provide the best overall throughput.
- Minimum Unicast Rate. Changing this is less important than it is for 2.4 GHz as the long tail of coverage seen with a 1 Mb/s rate on 2.4 GHz is much more pronounced than 6 Mb/s is on 5 GHz. However, I often find that using 12 Mb/s on 5 GHz yields the best roaming results. For good roaming, you will also want to design for good overlap of coverage at this data rate.
- Candidates Channel. In most cases, leaving this at default of All is the best choice. However, if you have clients that do not support DFS channels, you can select non-DFS preferred. Or, if you are deploying outdoors and want to reserve some 5 GHz channels for PtMP radios and others for WiFi APs, you can set the list of channels from which the AP's can choose here.
- Airtime Fairness. I am ambivalent about Airtime Fairness in 5 GHz. Previous to the prevalence of 802.11ac clients in 5 GHz, this feature did offer good separation of client speeds, preventing the slower 802.11a clients from forcing 802.11n clients to their speed. 802.11ac, however, has measures built in, like better block acknowledgment, to prevent this from being an issue. And, it is possible for Airtime Fairness to actually slow down 802.11ac clients. My recommendation is to leave it disabled.



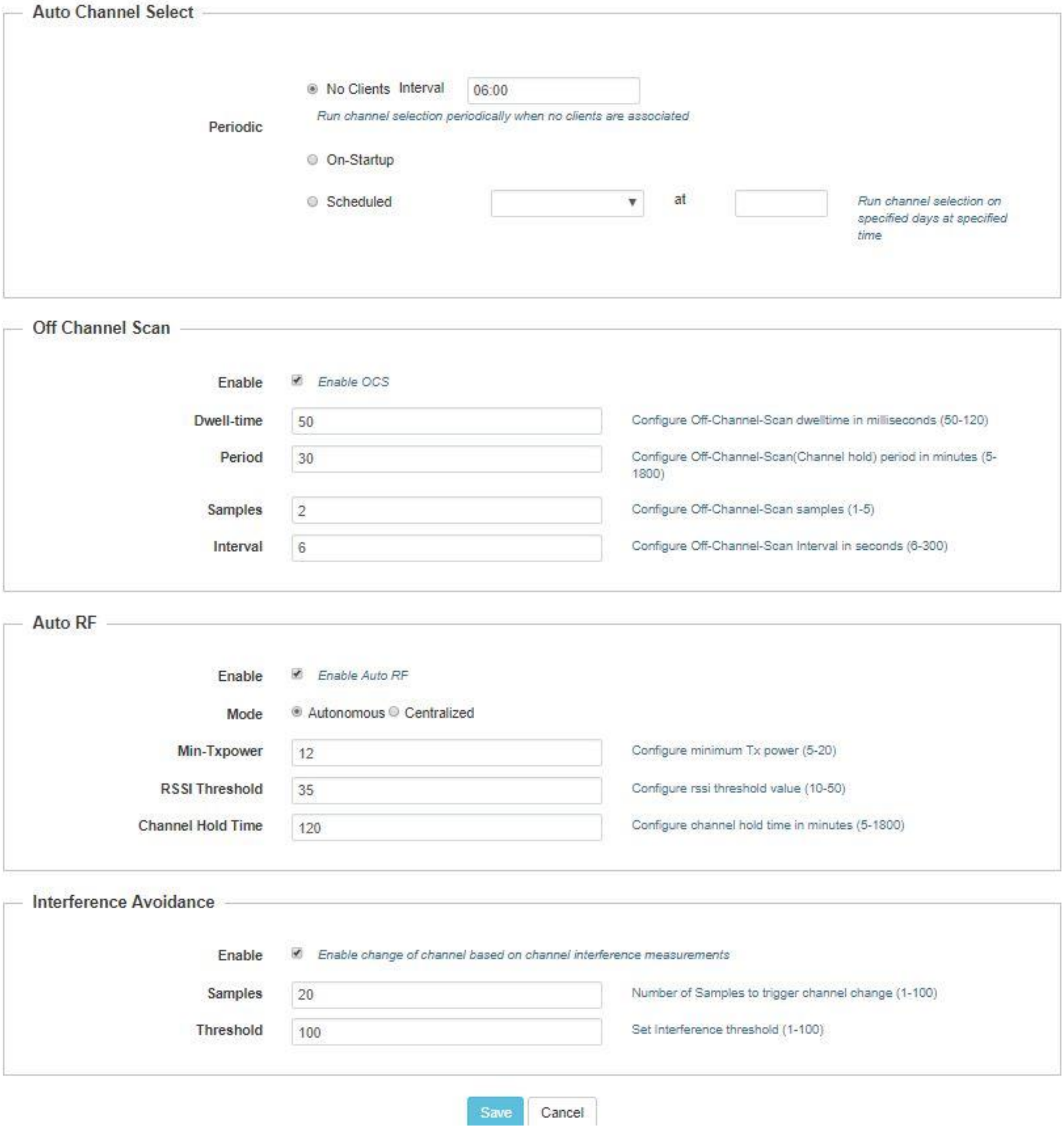
Edit Radio

Radio

Enable	☑ *Enable operation of this radio*	
Channel	Automatic	*Primary operating channel*
Channel Width	20MHz	*Operating width of the channel*
Transmit Power	Auto	Radio transmit power in dBm (4 to 30; Subject to regulatory limit)
Beacon Interval	100	Beacon interval in mSec (100 to 3400)
Minimum Unicast rate	6	Configure the minimum unicast data rate (Mbps)
Multicast data rate	Highest Basic	Data-rate to use for transmission of multicast/broadcast packets
Airtime Fairness	□ *Enable Airtime Fairness*	
Candidate Channels	All	
Mode	default	All modes clients are allowed

- Automatic Channel Select. Enable, choosing “No Clients” and the default of 6 minutes.
- Enhanced Roaming. Do not enable.
- Off-Channel Scan. Enable, using the default settings.
- Auto RF. Enable, using the default settings.
- Interference Avoidance. Enable, using the default settings.

Be sure to save your changes.



Auto Channel Select

Periodic
● No Clients Interval 06:00
Run channel selection periodically when no clients are associated
○ On-Startup
○ Scheduled ▼ at *Run channel selection on specified days at specified time*

Off Channel Scan

Enable ☑ *Enable OCS*
Dwell-time 50 Configure Off-Channel-Scan dwelltime in milliseconds (50-120)
Period 30 Configure Off-Channel-Scan(Channel hold) period in minutes (5-1800)
Samples 2 Configure Off-Channel-Scan samples (1-5)
Interval 6 Configure Off-Channel-Scan Interval in seconds (6-300)

Auto RF

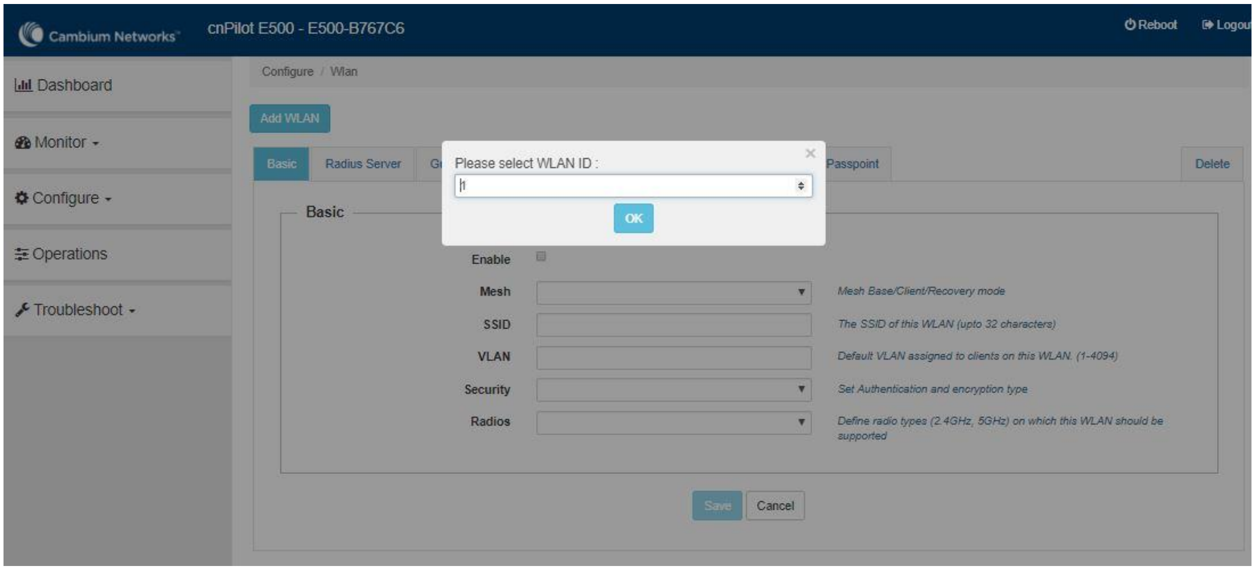
Enable ☑ *Enable Auto RF*
Mode ● Autonomous ○ Centralized
Min-Txpower 12 Configure minimum Tx power (5-20)
RSSI Threshold 35 Configure rssi threshold value (10-50)
Channel Hold Time 120 Configure channel hold time in minutes (5-1800)

Interference Avoidance

Enable ☑ *Enable change of channel based on channel interference measurements*
Samples 20 Number of Samples to trigger channel change (1-100)
Threshold 100 Set Interference threshold (1-100)

Configure WLAN Settings

Next click on WLAN under the Configure menu. Here is where you will create your WLANs. First, you must Add a new WLAN by clicking on the Add WLAN button at the top. If this is the first WLAN, choose "1" for the WLAN ID. If it is not the first, choose the next available number. This is not the name that will be assigned to the SSID.



Please select WLAN ID : 1

Basic

Enable □

Mesh — Mesh Base/Client/Recovery mode

SSID — The SSID of this WLAN (upto 32 characters)

VLAN — Default VLAN assigned to clients on this WLAN. (1-4094)

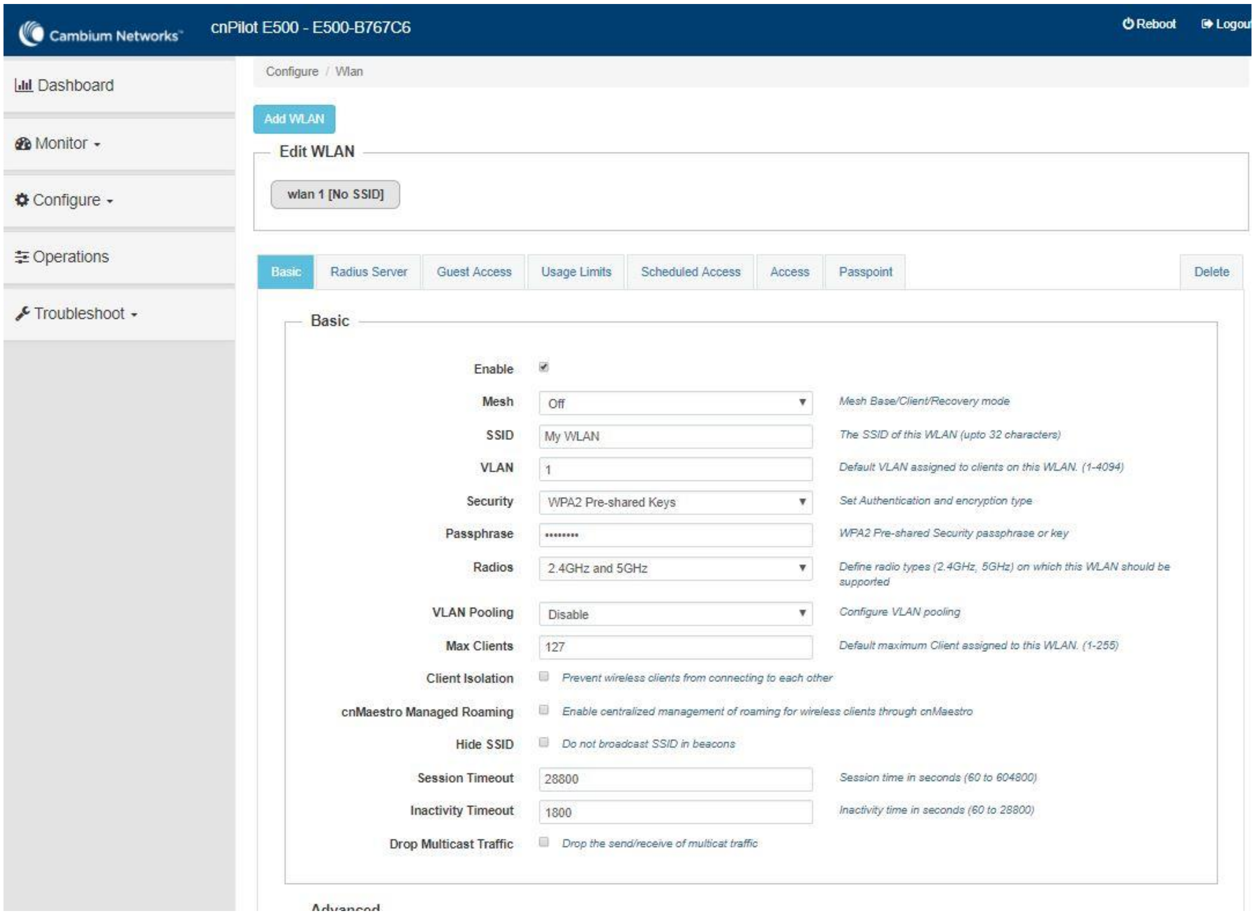
Security — Set Authentication and encryption type

Radios — Define radio types (2.4GHz, 5GHz) on which this WLAN should be supported

Select OK and begin configuring the WLAN settings. I will only cover the most common settings here and will not go into all of the possible options.

Basic

- Enable. If you are just preparing an AP configuration but you are not ready for the WLAN to be live yet, you can choose to not enable the WLAN at this time, saving that for later.
- SSID. Choose the SSID that will be broadcast for this WLAN.
- VLAN. You can assign a VLAN to this WLAN. By default, the VLAN is set to 1 and is untagged. However, you can select any valid VLAN ID and also choose to tag traffic from the WLAN as it passes to the Ethernet port.
- Security. Choose your security/authentication settings. Most commonly used are Open, WPA2-PSK, and WPA2-Enterprise. I will not go into WPA2-Enteprise in this document as that also requires configuration of a RADIUS server.
- Client Isolation. This feature prevents clients from communicating with each other and is very useful on a WLAN used for Guest traffic.

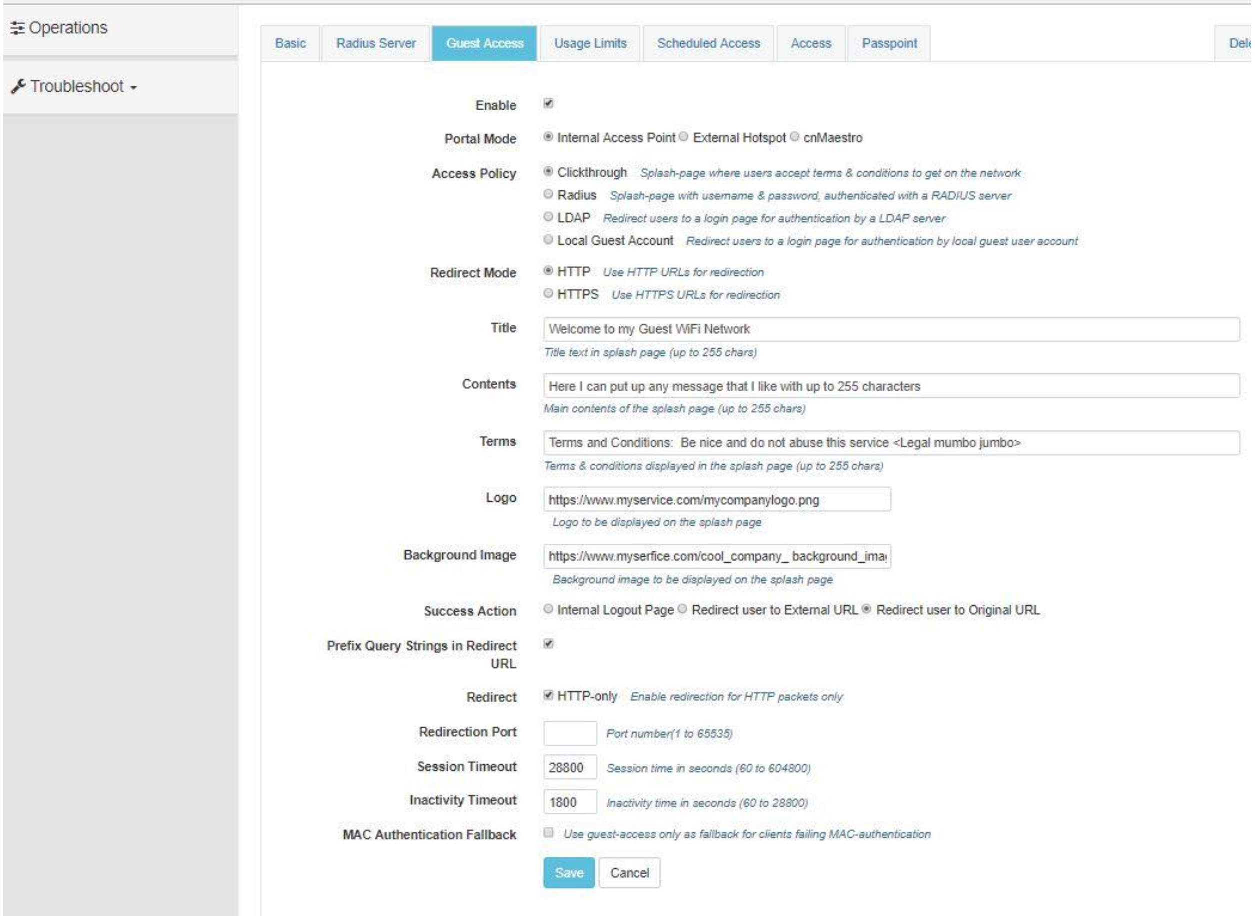


Enable	☑	
Mesh	Off	Mesh Base/Client/Recovery mode
SSID	My WLAN	The SSID of this WLAN (upto 32 characters)
VLAN	1	Default VLAN assigned to clients on this WLAN. (1-4094)
Security	WPA2 Pre-shared Keys	Set Authentication and encryption type
Passphrase	••••••••	WPA2 Pre-shared Security passphrase or key
Radios	2.4GHz and 5GHz	Define radio types (2.4GHz, 5GHz) on which this WLAN should be supported
VLAN Pooling	Disable	Configure VLAN pooling
Max Clients	127	Default maximum Client assigned to this WLAN. (1-255)
Client Isolation	□	Prevent wireless clients from connecting to each other
cnMaestro Managed Roaming	□	Enable centralized management of roaming for wireless clients through cnMaestro
Hide SSID	□	Do not broadcast SSID in beacons
Session Timeout	28800	Session time in seconds (60 to 604800)
Inactivity Timeout	1800	Inactivity time in seconds (60 to 28800)
Drop Multicast Traffic	□	Drop the send/receive of multicat traffic

Guest Access

If you choose to use this WLAN for Guest traffic, select the Guest Access tab and configure the WLAN further.

- Enable. This selection will enable the Guest features on the WLAN.
- Portal Mode.
  - Internal Access Point. This option allows you to build a simple Guest Portal, filling in the Title, Contents, Terms, Logo, Background Image, and choose how to redirect after a successful login. For a single AP, this is a quick and easy method of creating a Guest Portal, although not as configurable as an External Hotspot or using cnMaestro.
  - External Hotspot. This option allows you to redirect to an external hotspot service.
  - cnMaestro. This option allows you to use a very customizable Guest Portal on cnMaestro. However, I assume that if you are configuring the APs via the AP GUI, you are not utilizing cnMaestro.



Enable ☑

Portal Mode ● Internal Access Point ○ External Hotspot ○ cnMaestro

Access Policy
● Clickthrough *Splash-page where users accept terms & conditions to get on the network*
○ Radius *Splash-page with username & password, authenticated with a RADIUS server*
○ LDAP *Redirect users to a login page for authentication by a LDAP server*
○ Local Guest Account *Redirect users to a login page for authentication by local guest user account*

Redirect Mode
● HTTP *Use HTTP URLs for redirection*
○ HTTPS *Use HTTPS URLs for redirection*

Title: Welcome to my Guest WiFi Network
Title text in splash page (up to 255 chars)

Contents: Here I can put up any message that I like with up to 255 characters
Main contents of the splash page (up to 255 chars)

Terms: Terms and Conditions: Be nice and do not abuse this service <Legal mumbo jumbo>
Terms & conditions displayed in the splash page (up to 255 chars)

Logo: https://www.myservice.com/mycompanylogo.png
Logo to be displayed on the splash page

Background Image: https://www.myserfice.com/cool_company_ background_ima
Background image to be displayed on the splash page

Success Action ○ Internal Logout Page ○ Redirect user to External URL ● Redirect user to Original URL

Prefix Query Strings in Redirect URL ☑

Redirect ☑ HTTP-only *Enable redirection for HTTP packets only*

Redirection Port: *Port number(1 to 65535)*

Session Timeout: 28800 *Session time in seconds (60 to 604800)*

Inactivity Timeout: 1800 *Inactivity time in seconds (60 to 28800)*

MAC Authentication Fallback ☐ *Use guest-access only as fallback for clients failing MAC-authentication*

Save Cancel

Be sure to save your settings.

At this point you are ready to go. If the AP was not connected to your live network, you can do so now.