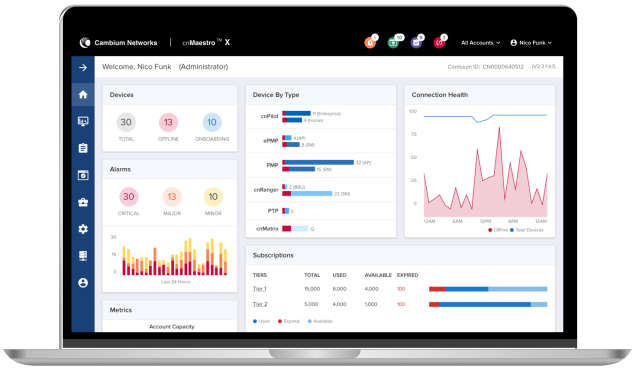
Wi-Fi Deployments in Multi-Dwelling Units (MDU)

CAMBIUM NETWORKS OFFERS A COMPLETE SOLUTION FOR MULTI-DWELLING UNITS, FEATURING MULTI-GIGABIT CONNECTIONS AND TOTAL INDOOR/OUTDOOR WI-FI COVERAGE. THANKS TO POWERFUL AND COST-EFFECTIVE TECHNOLOGIES, RESIDENTS AND GUESTS CAN STAY CONNECTED THROUGHOUT YOUR PROPERTY—AND YOU CAN KEEP YOUR FOCUS ON CORE BUSINESS NEEDS.

MDUs HAVE WI-FI NEEDS THAT ARE UNIQUE in in that they combine the elements of public Wi-Fi with private Wi-Fi. Furthermore, it is imperative that the Wi-Fi network provide adequate performance and be easy to access. MDUs vary in type and size, but the basic need is for good coverage, easy access, and separation of traffic. There are some variances in best practices between the different MDU types, but the basic design remains the same. In this document we will discuss each of the following topics:



Multi-tenancy isolates customer data, and encryption prevents visibility of communications between a customer and the cloud.

MDU Deployment Examples:

Apartments

Apartments are the most common example of MDUs and of all the examples that we will examine. This is the example with the highest user density. Depending on the size and complexity of the units, it may be possible to provide adequate coverage with traditional APs in hallways and common areas, covering more than one apartment per AP. However, a better design is to mount an AP within each unit.

One aspect of apartments that is quite important to a good Wi-Fi design is that there tends to be a fair amount of bleed through of Wi-Fi signal between units, both next to each other and from floor to floor.

Senior and Assisted Living

Senior living and assisted living facilities are an often overlooked MDU type. More and more are being built and those entering into these facilities are more active on the internet than ever before. Where Wi-Fi might not have been considered a necessity for this market in the past, it is now considered

a basic utility. These facilities can vary as much as apartments and can be considered nearly identical for Wi-Fi needs and design with the exception that there are generally more common areas and more need for guest access.

Townhouses

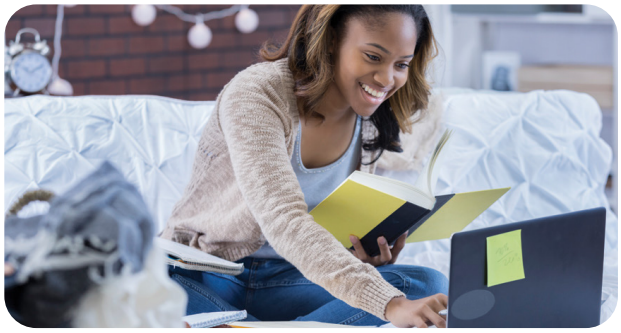
Townhouses tend to be much larger units with fewer of them connected to each other. For this reason, unlike apartments, townhouses tend to be subject to less bleed through of Wi-Fi signal from one unit to another and can possibly be best treated as single dwelling units.

Barracks

Military barracks can be considered as very similar to dormitories. Size and density of users are very similar. Also similar is the heavy use of Wi-Fi for gaming devices.

Student Housing

Student housing is a unique example of an MDU. The residents change often. The users make heavy use of Wi-Fi, perhaps the heaviest of all these examples. And, last but not least, the density of both users and devices is the highest of all of the examples. Student housing areas can vary from tiny to luxurious spaces, but they do tend to be packed closer together than apartments, meaning that Wi-Fi signal bleed through will be high.



Wi-Fi Needs for MDUs:

Residents

In each MDU case that we are examining, the residents are the most important. They also have the ability to provide their own Wi-Fi. The problem with this is, especially in the denser deployments, that when residents start to implement their own solutions, there tends to be more problems with interference. If you provide poor Wi-Fi for the residents, they will add their own. That will, in turn make Wi-Fi even worse for everyone. It is in your best interest, and that of the residents, to provide excellent Wi-Fi to everyone.

Accessibility

Access to the Wi-Fi network must be easy: easy to find, easy to connect, and easy to use. This includes all devices that residents use. That list is much longer than ever before with not only PCs and laptops, but also printers, TVs, Apple TV, Roku, Alexa, tablets, iPads, smart watches, refrigerators, thermostats, and surveillance cameras. Some of these devices utilize broadcast protocols such as bonjour and CUPS to advertise their services.

This means that you cannot enable Client Isolation as you would for a guest network.

Security

It is vital that each residential unit's network traffic be kept private. As we discussed previously, however, there is a real need to allow all devices within a residence to have free communications between them. Each residence needs to be treated as a unique and separate network. It is also important to prevent unauthorized users to access the network as they could take up bandwidth intended for the residents.

Guests

The choice to allow guest access should be considered, along with an implementation of how to limit that access to valid guest users and not just someone living or lurking close by. It is also important to limit guest access so that it does not impinge on bandwidth reserved for residents.

Wi-Fi Network Design:

The Traditional Design

Traditionally, Wi-Fi in MDUs has been provided by using a home Wi-Fi/router in each unit. At first, this might seem to make the most sense. Each dwelling unit will have its own SSID and its own subnet. Traffic remains separated between the units, providing security for the residents from each other. However, there are definite drawbacks to this approach.

With a different SSID for each unit, there will be a very large number of them visible from any location throughout the complex. This can be confusing to the residents. It is also a lot for the Managed Service Provider (MSP) to manage.

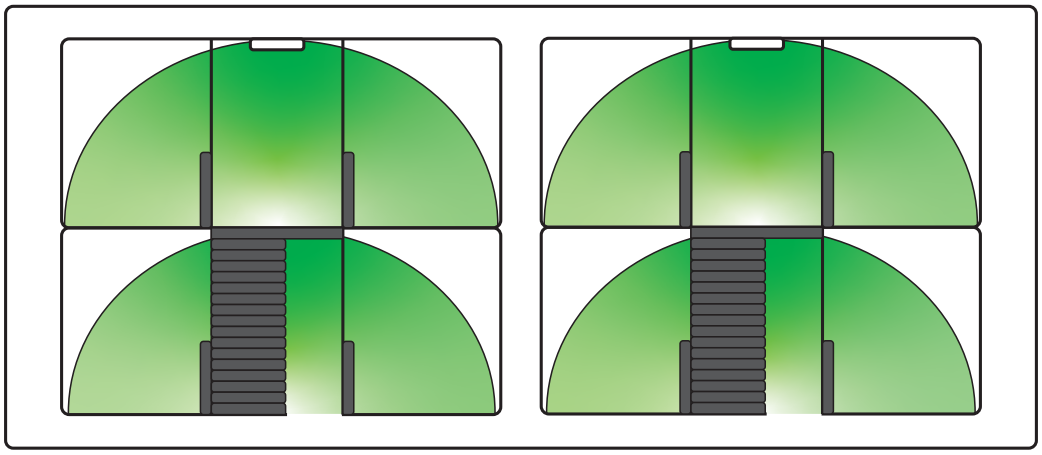
Coverage for each unit is provided by an AP within each unit. For dormitories and barracks, this is generally not a large concern. However, with apartments, senior living, and townhomes, there will be locations within a resident's unit where they will have better signal strength from the AP inside their neighbor's unit.

If Wi-Fi is to be provided to common areas, it will be necessary to have an additional SSID present in those areas. Keep in mind that for every SSID, beacons are broadcasted by each AP. With only 4 different SSIDs present on the same channel being seen by 4 different APs, over 50% of the airtime is used by these beacons alone. That means that ½ of the possible capacity is being used by beacons. It is always better to reduce the number of beacons to as few as it possible.

A Better Design

1. Cambium Networks offers a complete solution for multi-dwelling units, featuring multi-gigabit connections and total indoor/outdoor Wi-Fi coverage. Powerful and cost-effective technologies allow residents and guests to stay connected throughout a property—and allows network operators to focus on core business needs.
2. Cambium Networks enables you to create a better design, one that simplifies connectivity for residents, protects their security, maximizes airtime, and also eases network management for the MSP.
    c. Instead of deploying a separate SSID for each unit, use a single SSID for the entire complex. If APs are placed within each unit, they will provide coverage to neighboring tenants. Devices will connect to the best possible AP in all cases. Even common areas are provided for with this single SSID.

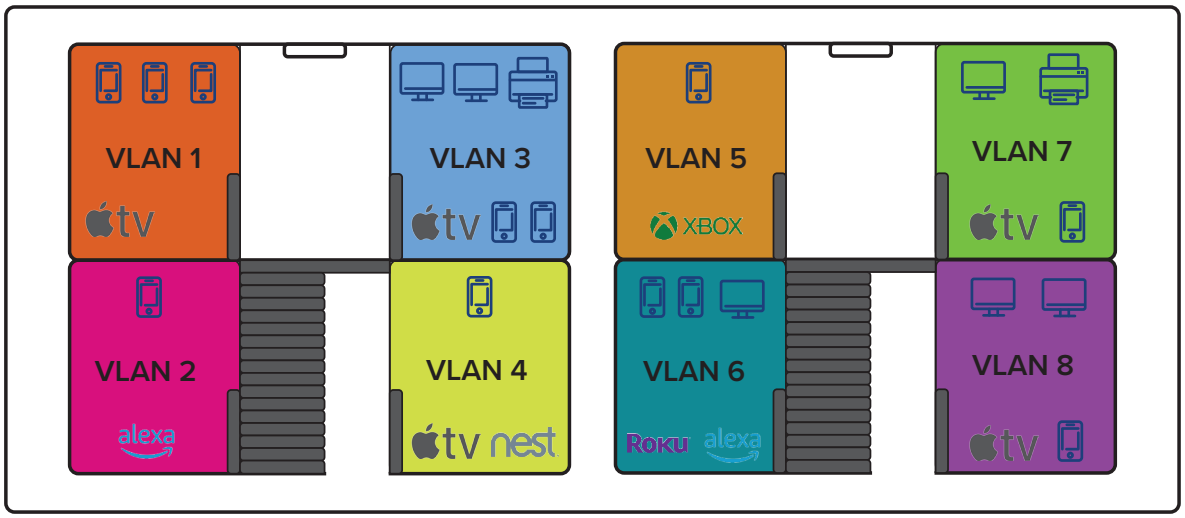
One Wi-Fi Network, Corner-to-Corner



d. Individual tenants receive a personal PSK, working on all their devices. cnMaestro™, Cambium Networks' cnMaestro X Cloud Management platform supports up to 1,024 unique PSKs natively and an unlimited number of PSKs with RADIUS integration.

e. MSPs should also separate traffic into a unique VLAN for each dwelling unit. All of the PCs, Apple TVs, smart watches, iPhones, etc. that are owned by a single residence are placed on the same VLAN. By doing this, residents can use their printers and can watch Netflix, but they cannot see their neighbors' devices and traffic.

Per-Tenant Secure Access for All Devices



f. For MDUs requiring Ethernet solutions, Cambium Networks' cnMatrix™ EX series is a feature-rich, enterprise-grade Ethernet switching solution. For an MDU requiring an application like VoIP handsets in living units, the EX series provides policy-based automation, auto-device segmentation, auto-policy wipe, is wireless aware and can be managed via the cloud or on-premises.

3. But how do you make this process simple? By offering cloud-managed access and visibility for service providers and their customers.

a. Centralized cloud management makes it easy to plan, deploy and oversee a property's connectivity. Each device features dedicated dashboards with common and centralized upgrades, zero-touch provisioning and device configuration workflows to minimize the learning curve for network managers.

a. Radius Authentication Dial-In User Service (RADIUS) is commonly used to provide centralized authentication, authorization and accounting (AAA) for dial-up, virtual private networks and fixed wireless network access.

a. The key is to use a captive portal in conjunction with RADIUS MAC authentication and dynamic VLANs. When a resident first connects to the Wi-Fi network, they should be redirected to a captive portal where they can be verified as a resident. The captive portal should then allow residents to self-register their other devices. Not all Wi-Fi devices have a browser that can use a captive portal, so it is important to provide a method for adding those devices into the system. The captive portal then updates the RADIUS database, assigning a single and unique VLAN to all of the devices registered for a single residential unit. Once this is complete, a CoA (Change of Authentication) message is sent to the AP where the user is connected telling the AP to

disconnect the client device. The device will immediately attempt to reconnect, but this time it will be assigned to the VLAN specified by the RADIUS server. All devices are now connected on their own private network within the same SSID. By placing each VLAN within a unique subnet, the network operator can also provide all of the bandwidth restrictions desired as well as firewall services to each residence.

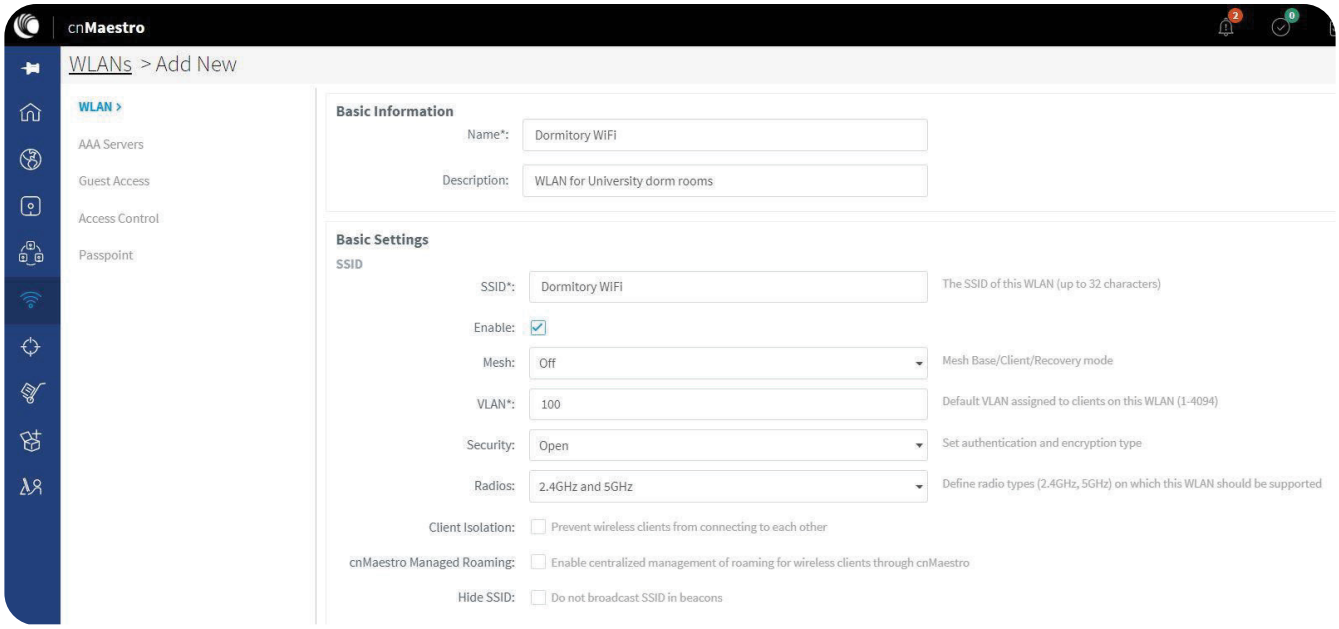
Registration Process

- Each new user connects to Wi-Fi with a browser capable device and is placed in “safe” VLAN
  - OAP passes MAC address to RADIUS server for authentication
  - RADIUS server allows authentication but retains default (safe) VLANID
- The user is redirected to captive portal and asked for login credentials
  - The captive portal updates RADIUS database with user device MAC and assigned a unique VLANID
  - User is given the opportunity to enter the MAC address of other devices, to include headless devices

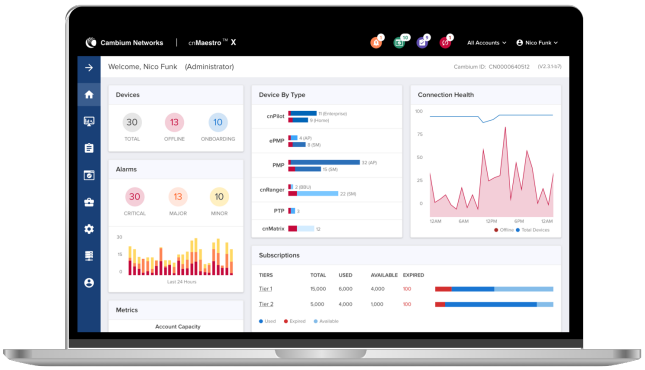
  - Added device MAC addresses are updated to RADIUS database along with dwelling unit VLANID
- CoA message sent to AP
  - User device disconnects and then reconnects with the new VLAN
  - All devices in a single dwelling unit share the same VLANID unique to that unit

Wi-Fi Access Point Configuration

In order to configure a Wi-Fi access point (AP) for this better design, you will need to configure the WLAN used specifically for RADIUS MAC authentication with CoA capabilities. The simple steps shown below for configuration are all done through the cnMaestro management system. While it is possible to also configure the same functions through the AP GUI, it makes more sense to also take advantage of the MSP features offered by cnMaestro such as reporting, multi-tenancy, API for interfacing with other systems (e.g., billing system integration, industrial systems management, etc.) and AP grouping.



cnMaestro X Multi-Tenancy



cnMaestro X, a simple yet sophisticated next-generation network management solution for Cambium Networks wireless and wired solutions, features advanced management capabilities. One advanced feature is the MSP dashboard, which allows MSPs to differentiate their brand to address specific submarkets in their service area. The multi-tier customization gives the MSP tenant cloud tools to create an additional layer of guest portal customization – all managed from the cloud. MSP views consolidate the MSP tenant statistics while allowing the MSP to drill down and support a tenant directly. This does not impact data from other tenants or end users on the system.

New WLAN

First, configure a new WLAN through the WLAN ➔ New WLAN screen within cnMaestro.

Do not enable Client Isolation as that will prevent communications between devices such as an Apple TV and the TV. We also do not recommend hiding the SSID as you want connecting to the Wi-Fi network to be as simple as possible for the residents. Remember, if it becomes difficult, residents will start to deploy their own Wi-Fi equipment. This, in turn, will denigrate the quality of the Wi-Fi experience for everyone else by adding interference and complexity.

When a VLAN is configured to be private, communication is limited within the VLAN by restricting traffic flow. Private VLANs and ePSK work together to create a secure network segment that maintains security between tenants while still allowing devices within the same secure VLAN to communicate. ePSK offers the ability to assign different PSKs to different VLANs and can be exported and distributed to users as needed.

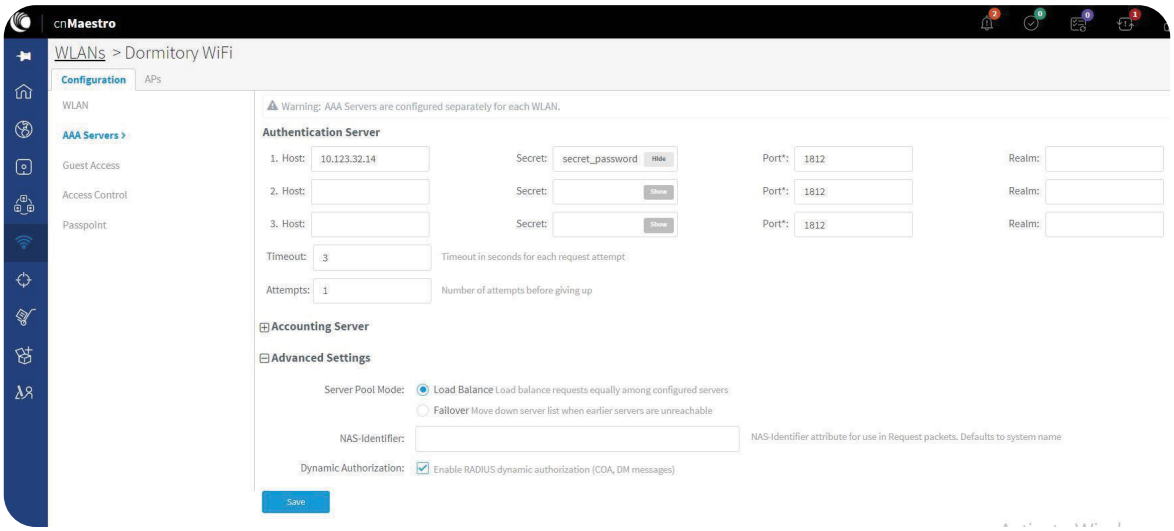
Note the use of a VLAN definition in this example. Clients that connect for the first time will be assigned to this VLAN. Configure this VLAN within your network to have access to the captive portal, and to support DHCP and DNS. However, do not allow Internet access. This will be a “safe” VLAN where first time users are temporarily housed until they complete the registration process. Then, all devices will connect to their own private network within the same SSID.

AAA Configuration

It will be necessary to utilize a RADIUS server for MAC authentication. The RADIUS server assigns a private VLAN to each tenant and ensures the tenant devices get the correct VLAN every time. At this time, cnMaestro does not provide a RADIUS server. However, there are various good options on the market, some of which are free to use such as FreeRADIUS (https://freeradius.org).

Cambium Networks Secure Gateway can be used in a variety of deployments and use cases, one of them being MDUs. It assists with user authentication and can dynamically provide per-use policies for bandwidth, QoS, traffic routing and security. It can be viewed as a combination of a Wi-Fi controller, router, DHCP server and firewall—all integrated into one solution. Essentially, is makes it possible to better manage traffic and bandwidth allocation, improves mobility and dramatically increases security.

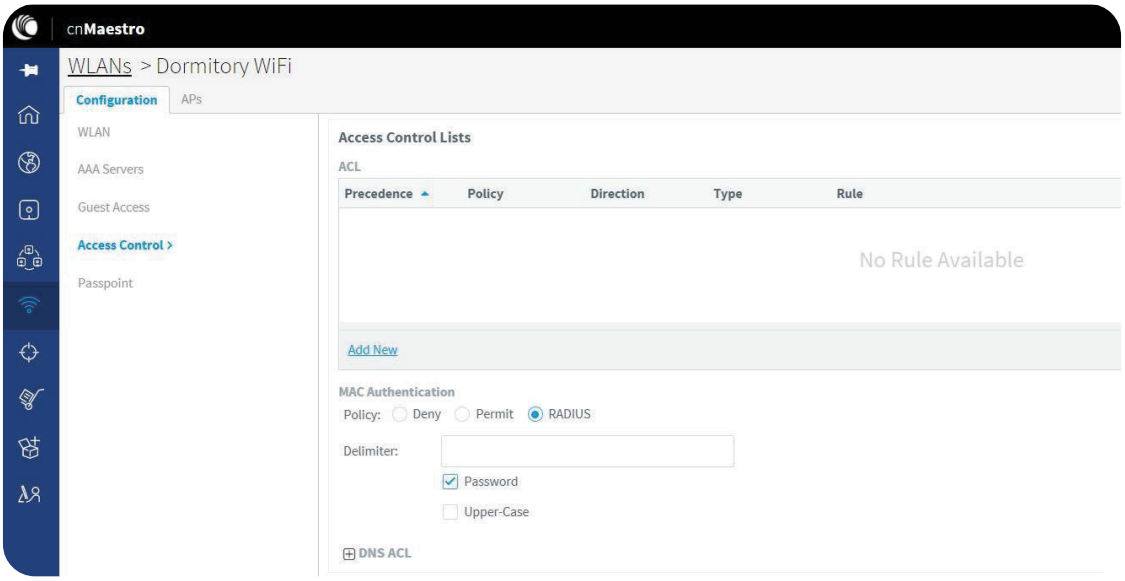
Configure the AAA service IP address, shared secret, and enable CoA within the WLAN on cnMaestro under the AAA Servers options for the WLAN that you are configuring.



Check the box for Dynamic Authorization. This will enable the APs to which this WLAN is assigned to understand and accept CoA and DM messages (Change of Authorization and Disconnect Message).

Guest Access

Next, you will want to configure Guest Access information for the WLAN, pointing to the external captive portal that will integrate with your RADIUS server. Although cnMaestro does offer a customizable Guest Access portal, it does not have the ability to fully integrate with a RADIUS server to the extent that is required for this type of deployment. There are options on the market for a captive portal that will integrate with Cambium Wi-Fi APs and cnMaestro. It is possible to use a captive portal as either a physical appliance or as a virtual machine, both with the RADIUS server built into it. If you have a capable staff, it may also be possible to write your own captive portal for this functionality.



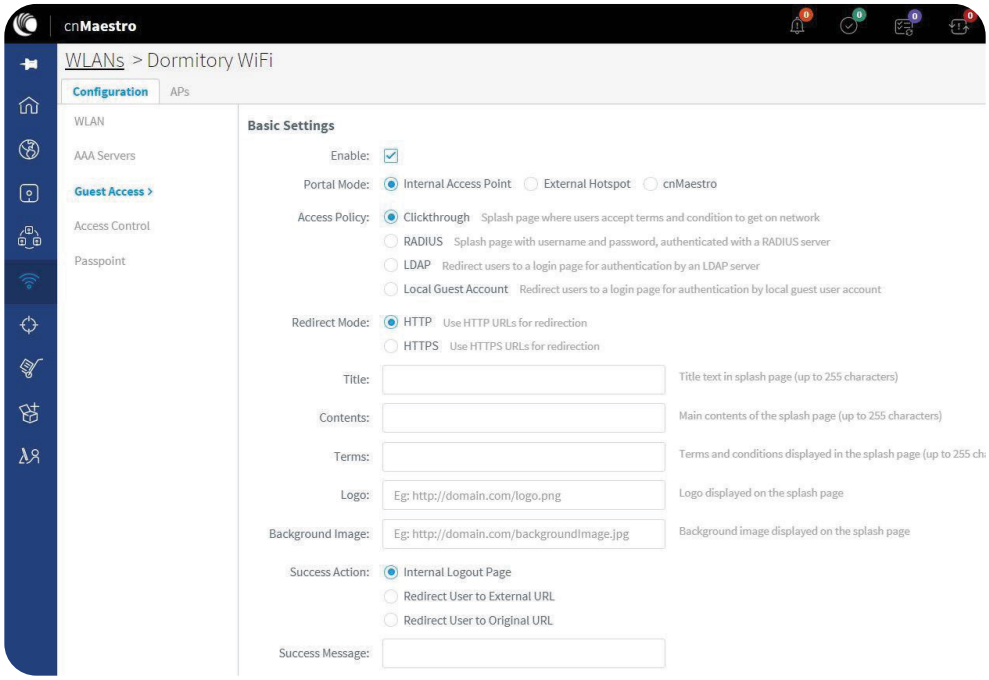
Configure the information needed to redirect first time users to the external captive portal.

In this example we show the use of HTTPS. While this is not strictly required, it is a good security practice. Tech savvy users will also insist on using HTTPS for any websites that request login information.

Access Control

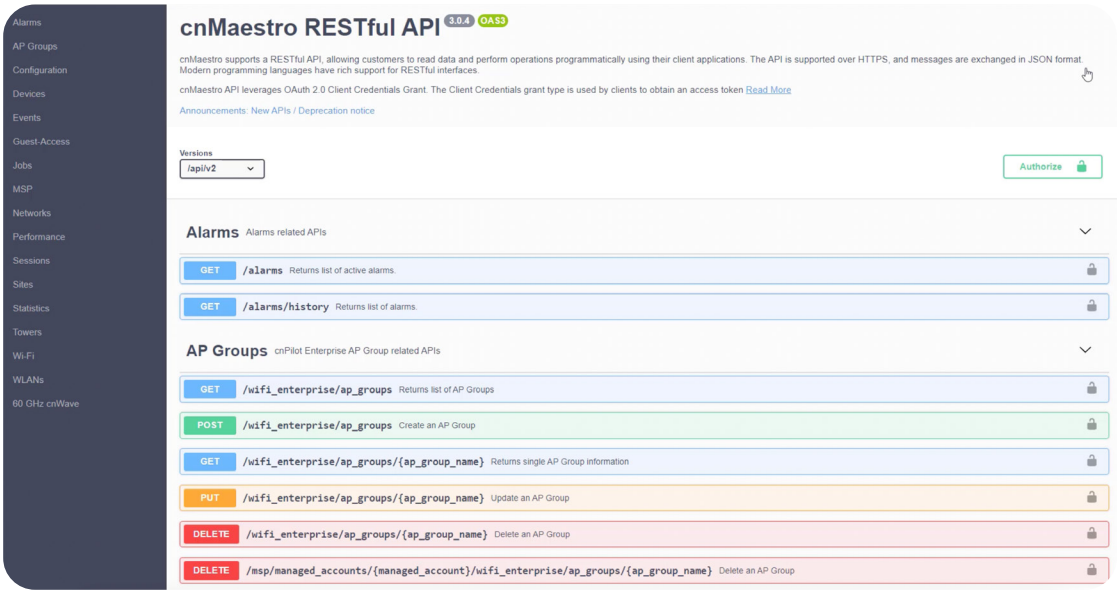
The last portion of the WLAN configuration is for Access Control and is found under WLAN ➔ Access Control for the specified WLAN. In this section, you will configure the WLAN to utilize RADIUS MAC authentication. This will tell the AP to send information such as the MAC address as well as the framed IP address to the RADIUS server.

Most RADIUS server implementations have the ability to access any typical delimiter (:, -, and even a space) as well as to accept both upper and lower case characters. If your implementation requires a specific delimiter or differentiates between upper and lower case characters, be certain to configure this form appropriately.



Application Programming Interface (API)

The cnMaestro X platform contains a rich set of RESTful telemetry and automation APIs. Most of the operations described above that are done from the cnMaestro dashboard can also be done programatically using these APIs.



Other Considerations and AP Models:

XV3-8 Wi-Fi 6 Access Point

The XV3-8 is an enterprise-grade, software-defined 8x8 multi-radio access point optimized for high-density and edge services. It features a total of five radios to deliver a next-generation network with high capacity and high density. Three data radios can be configured as two 5 GHz 4×4 plus one 2.4 GHz 4×4, or the two 5 GHz radios can be combined into a single 5 GHz 8×8 radio with the maximum power and performance of the 802.11ax standard. A dedicated network scanning radio provides continuous network monitoring to enhance security protocols, detailed network reports, and automatic RF optimizations. Add the Bluetooth Smart 4.1 IoT radio for BLE-based location services and you get a multi-radio, high-capacity Wi-Fi 6 AP designed for the most demanding networks in enterprise, education, retail and public venues.

For networks dominated by legacy 802.11ac client devices, the dual 5 GHz 4×4 mode will double network capacity to maintain high-bitrate services as density increases. As the devices migrate to the new Wi-Fi 6 standard based on 802.11ax, the XV3-8 SDR can be quickly converted into full 8×8 operating mode via a simple configuration change. No firmware change is required to support this mode.

XV2-2 Wi-Fi 6 Access Point

The XV2-2 is a dual-radio Wi-Fi 6 access point designed to deliver next-generation networks with edge

services at a value-based price. Wi-Fi 6 technology delivers higher network speeds and enables more connected devices at higher packet quality. Wi-Fi 6 brings a deterministic model to the radio frequency (RF) layer where the AP controls the client connections, including when to sleep, when to wake and how to transmit and receive packets. The XV2-2 is fully backward compatible with existing Wi-Fi technology and enables a massive growth of low power, low-bitrate IoT devices to add infrastructure intelligence into any market.

XV2-2T0 Outdoor Wi-Fi 6 Access Point

The XV2-2T0 outdoor Wi-Fi 6 access point covers significantly larger areas in campus networks and public Wi-Fi hotspot applications. Coupling Wi-Fi 6 technology with high efficiency antennas, the XV2-2T delivers up to a one-kilometer range as well as higher throughput at shorter ranges compared to competitive solutions. Covering more area per AP, network operators can save costs on equipment, cabling, installation, maintenance and access rights for outdoor Wi-Fi deployments. When paired with Cambium Networks' multi-gigabit 60 GHz cnWave solutions for Wi-Fi backhaul, network operators can blanket large areas with blazingly fast speeds – all wirelessly.

The XV2-2T's high-efficiency antennas deliver a maximum of 9 dBi and an average of 7 dBi gain over 360 degrees in 5 GHz, delivering maximum gain and minimum nulls. This enables the XV2-2T access point to deliver consistent coverage in all directions for optimal user experience.

XV2-2T1 Outdoor Wi-Fi 6 Access Point

The XV2-2T1 is a 90/120-degree sector version of the XV2-2T0 outdoor Wi-Fi access point. This AP will be more directional and designed for targeted coverage. XV2-2T1 APs are set to be released in mid-2022.

6 GHz & Wi-Fi 6E

Wi-Fi 6E is the implementation of the 6 GHz band for Wi-Fi. The "E" in "6E" stands for "extended," so 6 GHz and 6E are, in some instances, synonymous. Firstly, 6E includes 1200 MHz of clean, unlicensed spectrum. Regulatory bodies are endeavoring for thoughtful allocation of indoor and outdoor use cases of Wi-Fi 6E. Wi-Fi 6E excludes backward support for 802.11 a, n and ac, cleaning up the less efficient standards and making the most efficient use of that 1200 MHz of unlicensed spectrum. It can support up to 160 MHz channels, translating to significantly higher data rates. Historically, Wi-Fi has not been the best transport for Industrial Internet of Things (IIoT), although it has been viable for consumer and home networking, but the latency inhibited it from machine to machine, and 6E will address that issue. In the case of the FCC and other markets around the world, the use of an automatic frequency coordination (AFC) service will protect the incumbent users of licensed microwave.

With 6E, we can enable the digital home for work, study, recreation and connecting smart home devices. Wi-Fi 6E will be able to support augmented reality and virtual reality, advanced surveillance systems, digital classrooms, gigabit fixed wireless broadband connectivity, Industry 4.0 applications and more.

If you are making an investment in 6 GHz or 6E, you will want to consider the following:

- Do you have a software-defined access point?
- Do you have a tri-band Wi-Fi AP?

In the near term, 2.4 and 5 GHz are going to be the dominant bands, and you want to be able to allocate the computational horsepower and RF horsepower of that AP to take advantage of 2.4 and 5 GHz. At the same time, as the client population of 6E devices ramps up, you want to be able to allocate capacity on that AP to Wi-Fi 6E.

XE5-8 Wi-Fi 6E Access Point

The XE5-8 is a five-radio Wi-Fi 6/6E 8x8/4x4 access point (AP) designed to deliver high-density, future-proof performance for building next generation wireless networks. With five user servicing radios, the XE5-8 delivers the highest density Wi-Fi 6 solution in the industry. Wi-Fi 6E support extends the capacity of Wi-Fi into the 6 GHz band, more than tripling the wireless spectrum available. With high-speed software-defined radios, the XE5-8 enables seamless transition to Wi-Fi 6E with the ability to easily change from dual-band to tri-band (2.4 GHz, 5 GHz, 6 GHz) support when sufficient 6 GHz clients are available. The XE5-8 is fully backward compatible with existing Wi-Fi technology, enabling simultaneous support of new high speed clients, legacy clients, low-bitrate IoT devices, and more in a single wireless infrastructure.

XE3-4 Wi-Fi 6E Access Point

The XE3-4 is a tri-radio Wi-Fi 6/6E 4x4/2x2 access point (AP) designed to deliver future-proof performance and value for building next generation networks. Wi-Fi 6 delivers faster and more efficient wireless network connections than previous generation Wi-Fi technologies. Wi-Fi 6E extends the capacity of Wi-Fi into the 6 GHz band, more than tripling the wireless spectrum available. With a high speed software-defined radio, the XE3-4 enables seamless transition to Wi-Fi 6E with the ability to easily change from dual-band to tri-band (2.4 GHz, 5 GHz, 6 GHz) mode when sufficient 6 GHz clients are available.

The XE3-4 is fully backward compatible with existing Wi-Fi technology, enabling simultaneous support of new high speed clients, legacy clients, low-bitrate IoT devices, and more in a single wireless infrastructure.

Captive Portal

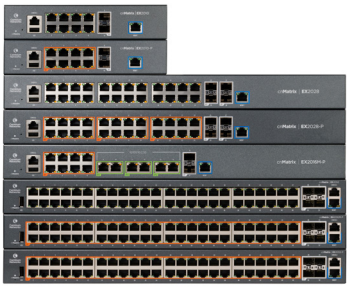
The captive portal plays an important role in this design. While cnMaestro does provide a guest access portal that can be customized in many ways, it does not currently offer the ability to allow users to self-register headless devices. For this, Cambium Networks recommends looking towards other products on the market. Solutions such as these provide not only the self-registration portal, but also an integrated RADIUS server and have been tested and proven to work with Cambium Wi-Fi APs.

RADIUS

A RADIUS server is also an integral part of this solution. There are many choices for a RADIUS server and any one of them should be usable as there are no aspects of this deployment that do not meet the standard functionality of a RADIUS server. FreeRADIUS (https://freeradius.org) is a free solution with significant documentation and forum support online but can be a bit daunting for the uninitiated.

Microsoft's NPS requires a license but offers a more friendly graphical interface.

Ethernet Switches and the Core Network



cnMatrix switches simplify network deployment and operation. When deployed with Cambium WLAN access points and the cnMaestro management system, network operators have an affordable, feature-rich, high-quality, unified, wired/wireless enterprise-grade network. Cambium Networks' cnMatrix enhances performance, security and end user satisfaction while reducing costs.

Additionally, policy-based automation (PBA) makes switching simple, secure and less error-prone. User-created policies automate switch and port configuration; these policies can be created via any management interface, and cnMaestro configures all switches simultaneously. PBA eliminates the burden of constant manual reconfiguration of "adds," "moves," and "changes" of network devices.

To manage it all is cnMaestro, a cloud-based or on-premises platform specialized for secure, end-to-end network lifecycle management. cnMaestro simplifies device management by offering full network visibility and offers a real-time view of the complete end-to-end network. The cloud-based cnMaestro comes with cnMatrix at no additional charge.

As dynamic VLANs will be used, there can be a significant number of VLANs that must be supported on the Ethernet switches deployed. Be certain to use Ethernet switches that can support as many VLANs as residential units for which they provide connectivity. Keep in mind that users may roam to any area of the complex. This means that at any one point in time, any Ethernet switch may need to support a larger number of VLANs than residential units that are connected directly to them. This is especially true of those switches that provide connectivity to APs covering common areas.

With multiple VLANs comes multiple IP subnets. Routing can either happen at the complex or be carried back to the MSP's core network. There is no reason to not use NAT, in fact this is likely to be the most commonly used method for providing IP addressing to all of the VLANs. Communications between the APs and cnMaestro is via TCP port 443, or HTTPS, which is not affected by NAT and is already allowed by any firewalls where internet access is required.

ABOUT CAMBIUM NETWORKS

Cambium Networks delivers wireless communications that work for businesses, communities and cities worldwide. Millions of our radios are deployed to connect people, places and things with a unified wireless fabric that spans multiple standards and frequencies of fixed wireless and Wi-Fi, all managed centrally via the cloud. Our multi-gigabit wireless fabric offers a compelling value proposition over traditional fiber and alternative wireless solutions. We work with our Cambium certified ConnectedPartners to deliver purpose-built networks for service provider, enterprise, industrial, and government connectivity solutions in urban, suburban, and rural environments, with wireless that just works.

cambiumnetworks.com