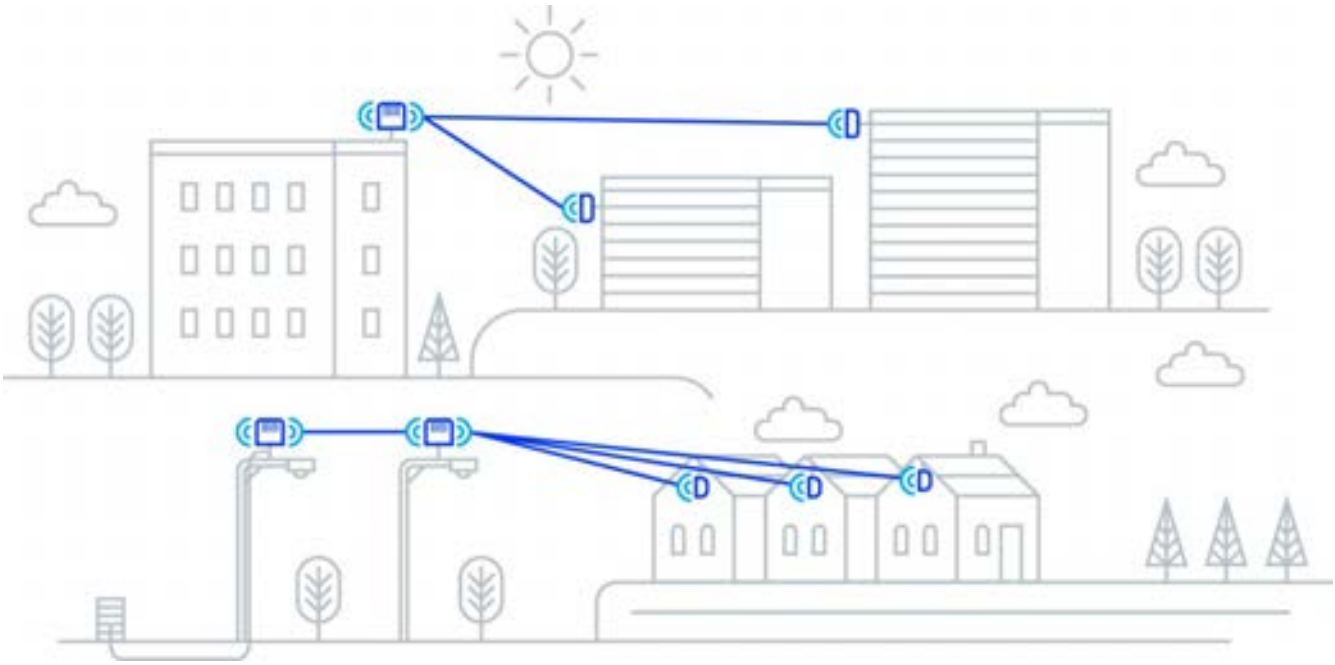


Altowav AltoPlex Platform

P421 User Guide

October 09, 2024

Version 2.8.0

Copyright, trademark, and legal information

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
— Reorient or relocate the receiving antenna.
— Increase the separation between the equipment and receiver.
— Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
— Consult the dealer or an experienced radio/TV technician for help.

Any modifications to this product which are not authorized by Altowav Inc. could void your authority to operate this equipment.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCT.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE ARE PROVIDED “AS IS” WITH ALL FAULTS. ALTOWAV DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL ALTOWAV OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OF DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF ALTOWAV HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Altowav would like to thank all of our staff for their efforts and expertise in development and implementation of the P421.

Regulatory statements

FCC Radiation Exposure Statement

The P421 device complies with FCC radiation exposure limits set forth for an uncontrolled environment. A minimum of 35 centimeters (14 inches) of separation between the P421 and all persons shall be maintained.

FCC Regulatory Statement

The P421 equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. For full Regulatory notices and statements, refer to the manufacturer and product as declared on the hardware label.

ISED Industry Canada Radiation Exposure Statement

IC Radiation Exposure Statement:

The P421 device complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. A minimum of 35 centimeters of separation between the P421 and all persons shall be maintained.

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Un minimum de 35 centimètres de séparation entre le P421 et toutes les personnes doit être maintenu.

ISED Industry Canada Regulatory Statement

The P421 device complies with Industry Canada licence-exempt RSS standard(s). This device contains license-exempt transmitter(s)/receivers(s) that comply with Innovation, Science and Economic Development Canada's license-exempt RSS(s). Operation is subject to the following two conditions:

(1) This device may not cause interference.

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

This device is not to be operated on aircraft except for the conditions listed in ISED RSS-210 Annex J.

Cet appareil contient des émetteurs/récepteurs exempts de license qui sont conformes aux CNR exempts de license d'Innovation, Sciences et Développement économique Canada. Son fonctionnement est soumis aux deus conditions suivantes :

(1) Cet appareil ne doit pas causer d'interférences.

(2) Cet appareil doit accepter toute interférence, y compris celles qui peuvent entraîner un fonctionnement indésireable de l'appareil.

Cet appareil ne doit pas être utilisé à bord d'un avion, sauf dans les conditions énumérées dans ISDE RSS-210, annexe J.

Revision history

Revision	Version
Initial release of the P421.	10/09/2024

Contents

P421 User Guide overview

Thank you for choosing the Altowav AltoPlex platform for your fixed-point networking solution. This user guide describes installation, configuration and operations for the P421 devices.

This guide is intended for network and system administrators who will install, configure, and manage Altowav networks using P421 devices.

This guide includes instructions for the installation, configuration and management of P421 devices using the WebUI. Other methods of device and network management, such as the Command Line Interface (CLI), REST API and the AltoCommand network management tool, are mentioned, but detailed instructions are not provided.

It is assumed readers are familiar with:

- Basic networking concepts.
- Routing and switching in networks.
- Specific network practices, operations and settings at the installation.
- The topology of the network being installed and managed.

Additional Documents

Further information about the P421 devices:

- For general technology specifications, see altowav.com/technology/
- P421 Quick Start.pdf
- P621 User Guide.pdf
- Altowav AltoCommand User Guide.pdf
- The Altowav Gen3 Platform also provides a REST API for smooth integration of your preferred network monitoring tools: REST API Usage Guide

Additional help

Altowav is committed to providing our customers with high quality technical support.

Web	support.altowav.com
E-mail	support@altowav.com

Introduction

Designed to help service providers deliver an excellent customer experience while managing costs, the AltoPlex platform utilizes carrier-grade gigabit connectivity to provide wireless network access. The platform enables highly customizable network management without the need for a centralized controller.

The AltoPlex platform delivers the superior performance and rich feature set promised by 802.11ay, with a lower cost and simplified management, as compared to our competitors in the 60 GHz solution marketplace.

A comparison of the Altowav Gen2 (802.11ad-based) and AltoPlex (802.11ay-based) devices shows some significant improvements.

	Altowav Gen2 (11ad-based)	**AltoPlex (11ay-based)**
60 GHz channels supported	3	4
Maximum goodput/ channel	1.8 Gbps	3.6 Gbps
MAC protocol	CSMA (contention-based)	TDMA
Channel symmetry	Adaptive	Fixed 50:50
Maximum clients per sector	8	15 (+1 DN link)
Data plane	Native Layer 2/transparent	Native Layer 2/transparent

With the AltoPlex platform, service providers can deploy and manage small to very large networks cost-effectively, and support many applications including:

- Gigabit fixed-wireless access (FWA).
- Wireless GPON.
- Surveillance camera connectivity.
- Smart city / smart pole distribution.
- Garden-style multi-dwelling unit distribution.
- High-speed data offload.

The AltoPlex platform includes a REST API, providing the flexibility for network administrators to use the monitoring and management systems of their choice.

P421 Installation and Configuration

Network topology design and deployment

The P421 has a weatherproof form factor with wireless coverage for 90° sector and a single RJ45 port. As with other AltoPlex devices, they require stable power, secure mounting, and a clear line-of-sight (LOS), to form a wireless connection.

The P421 is designed to operate in a point-to-point deployment with other P421s.

About AltoPlex wireless links

- 60GHz wireless links rely on clear line of sight (LOS).
- Configure P421 wireless links to other units through WebUI settings. Links between nodes are configured by using the DN link auto-configuration feature, or manually by configuring the **DN responder** setting.
- Weighted MCS levels are a good performance metric for the AltoPlex products. Power control in the P421 adjusts automatically to drive optimal MCS levels.

P421 — General information

Use this information to determine how best fit the P421 into your specific network design.

Throughput: 1.9 Gbps symmetrical.

Range: Expected maximum range for a P421-to-P421 link:

- MCS 9: up to 250 meters
- MCS 12: up to 150 meters

Scan range: 90° azimuth (-45° to 45°) for a single wireless sector. 17.5° elevation (-12.5° to 5°) range. Mounting hardware provides additional aiming flexibility.

Forming DN links with the P421: Use the DN link auto-configuration feature to configure DN links, which will automatically configure the DN responder with the correct link to the DN initiator as well as the channel, Golay index, and polarity.

Note: If the DN link auto-configuration feature is not used, both ends of the distribution node link must be manually configured prior to installation to have **DN Responder**, **Channel**, **Golay index**, and **Polarity** set.

Channel (1-4): Select a single channel.

Golay (1-3): Select a single Golay code. Use different Golay codes to mitigate co-channel interference when AltoPlex distribution nodes are set to the same channel and are within range of each other.

Polarity (odd or even): Polarity is a mechanism of TDMA used in determining when to transmit or receive during a timing cycle. It plays a critical role in TDMA operation.

GPS: Used for location and synchronization.

Deployment for common topologies

Altowav recommends creating a detailed network design and deployment plan with specific device, network and location information.

Considerations for all deployments:

- Keep in mind performance and operational characteristics of the P421 for range, and throughput, as listed above.
- Follow D621 Installation and guidelines.

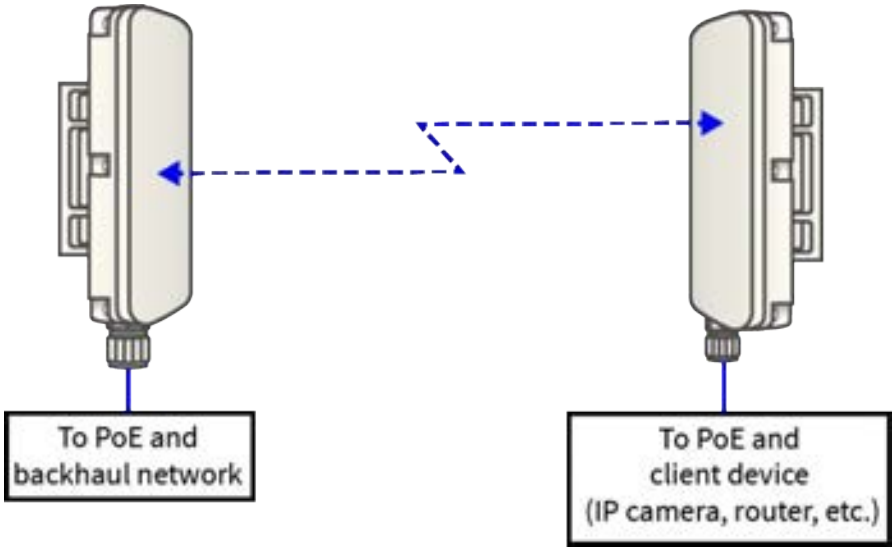
Point-to-point deployment

Point-to-point deployments involve either one distribution node and one client node, or two or more distribution nodes linked together in a serial fashion. Considerations for Point to Point (PtP) deployments:

- Select the best role for each end of the link, according to its planned function in the network. At least one P421 in the PtP link must be configured as a distribution node.

Simple point-to-point topology between two P421s

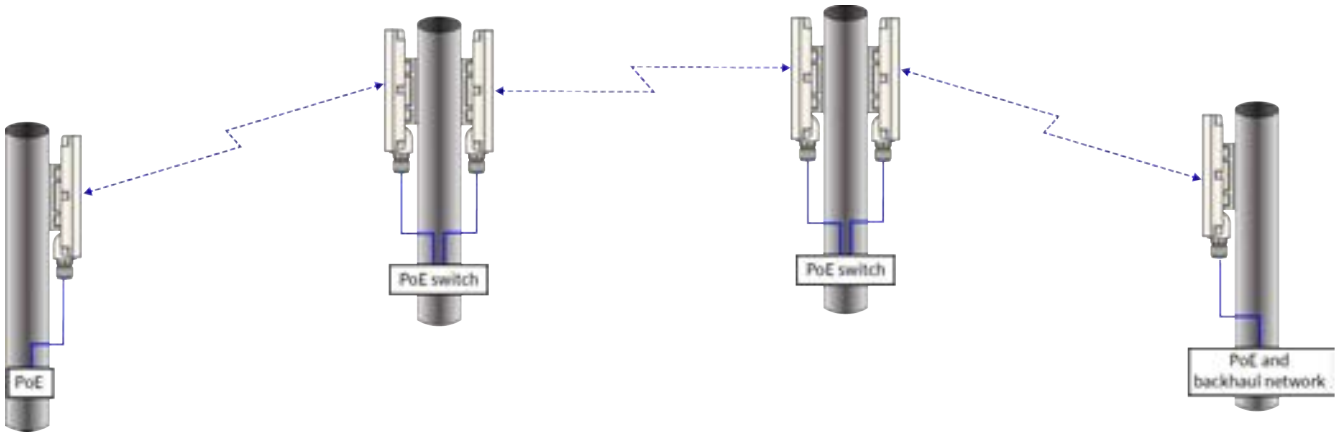
The following diagram demonstrates a simple PtP topology between two P421s.



Simple point-to-point topology involving to P421s

Point-to-point topology with multiple P421s

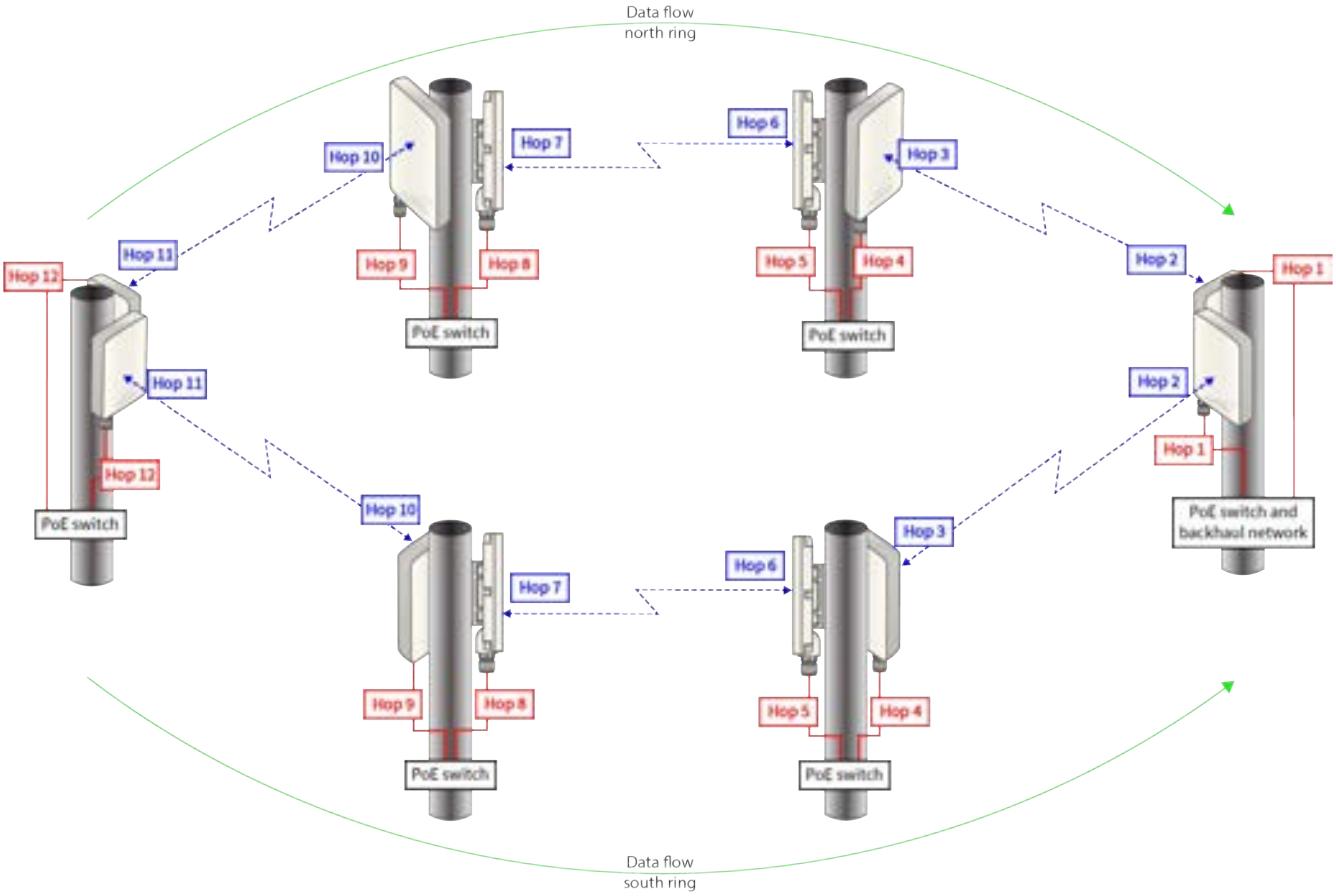
The following diagram demonstrates several P421s linked together in a serial fashion.



Point-to-point topology with multiple P421s

Ring deployment

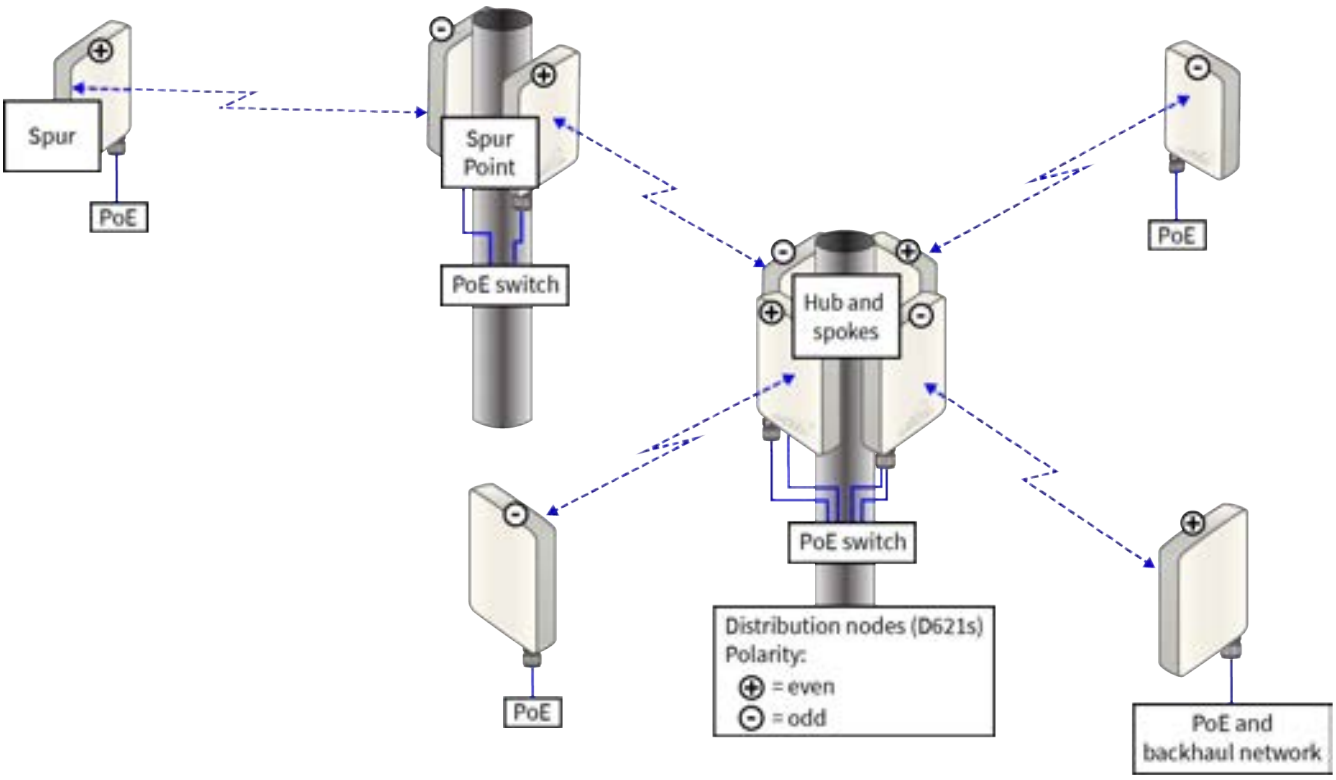
A ring deployment is a standard topology for AltoPlex deployments, and can be used to provide redundant backup network connections by utilizing Rapid Spanning Tree Protocol.



Ring topology utilizing Rapid Spanning Tree Protocol

Spur or Spoke Deployment

A spur or spoke deployment extends the reach of a distribution network. At least two P421s are required at the spur switch point that extends distribution to a wider azimuth range.



A hub-and-spoke topology with an attached spur

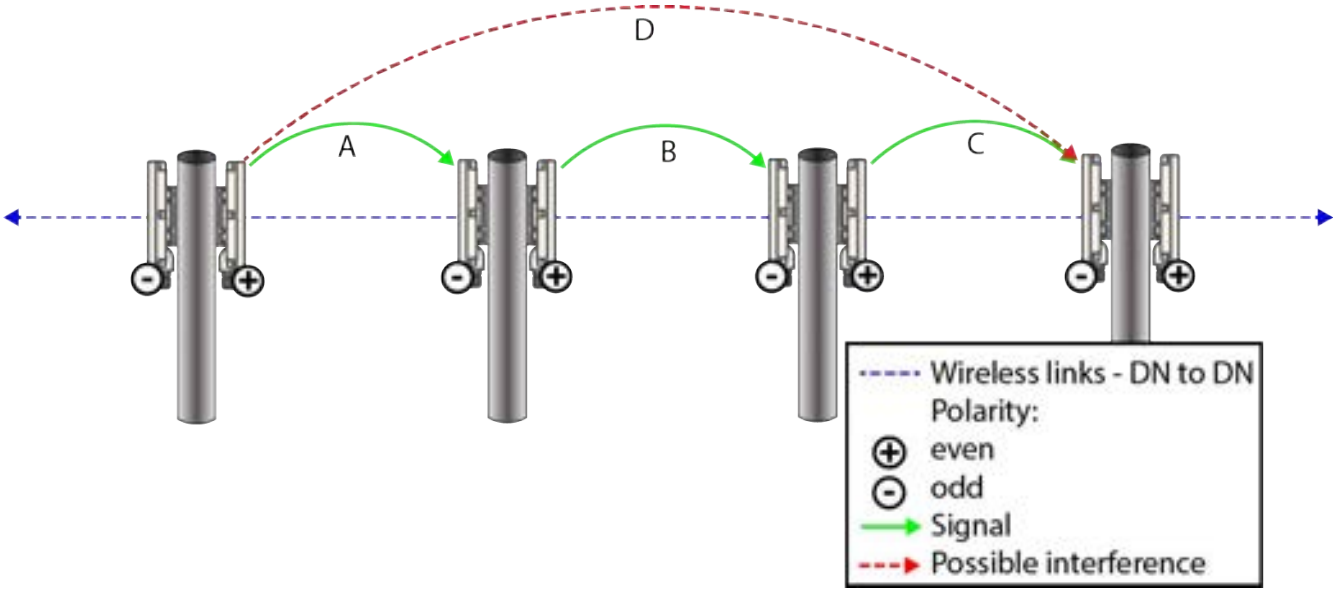
Design Issues to Avoid

The following describe common problems with design issues for 60GHz networks running on 802.11ay-based technology.

Issue: P421s in a straight line and too close together

An example of this is three or more P421 links in a line. In this configuration, a signal can be far reaching and cause interference to an unintended endpoint. Straight line interference is more impactful for short link distances.

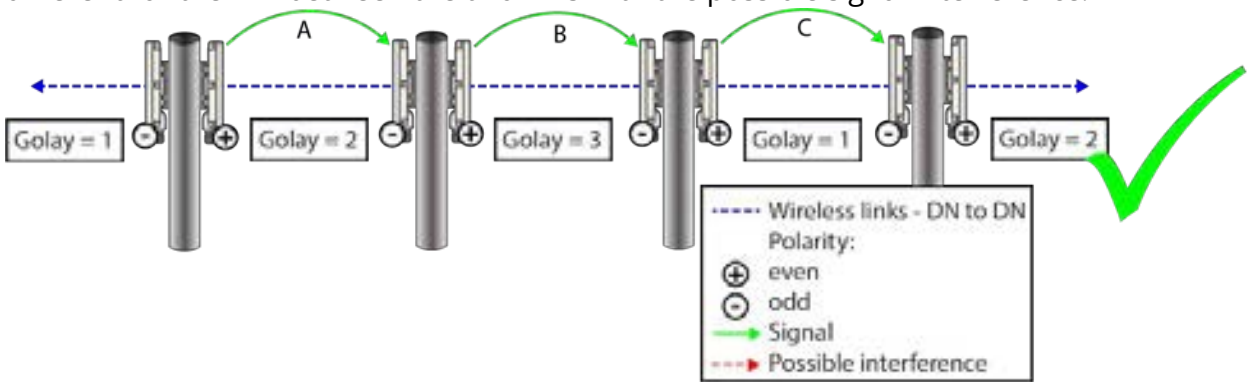
The diagram below shows even-polarity transmission in the same channel. In this case, signal A, can also cause a signal D that may interfere with an unintended endpoint such as interference.



Issue: Straight line interference

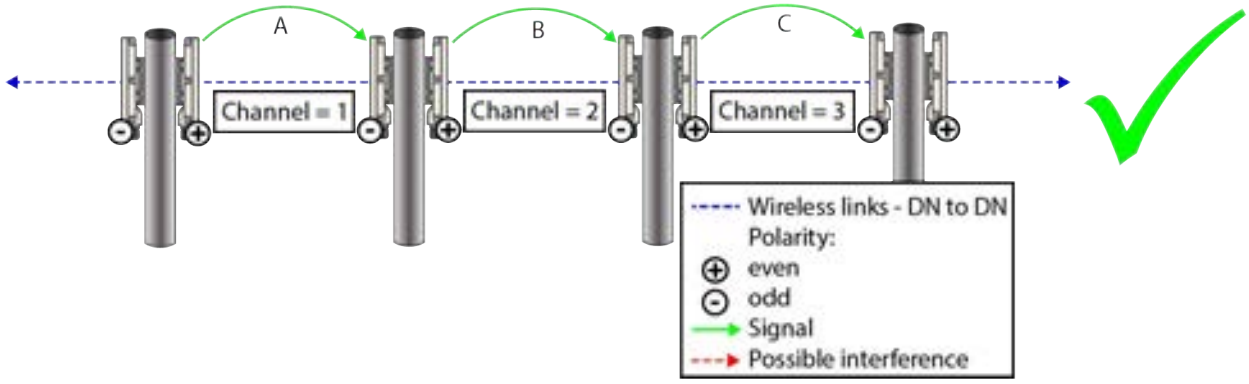
Solutions:

- **Set the Golay index (1-3) for both ends of each link.** Make sure that the Golay index is different for the link between the two DNs with the possible signal interference.



Using Golay codes to address straight-line interference

- **Less optimal solution:** Use different channels (1-4) between the distribution nodes. This provides a reliable solution, if network design and short link distances require it. However, in general practice the same channel is used in straight line formation to avoid adjacent sector interference and provide more flexible options for channel selection on adjacent sectors.



Using different channels to address straight-line interference

Preparing for installation

The P421 installation instructions include:

- Box contents, mounting options and PoE injector options.
- Functional description.
- Network design information required.
- Bench configuration steps.
- P421 on-site installation steps.

Box contents

- P421 device.
- IP67 cable gland.
- Indoor Power over Ethernet (PoE) injector:
  - Power supply:
    - Altowav Part Number: 1420-3016-0480.
    - Vendor: Procet.
    - Vendor Number: EN15GF.
  - Power cord.
- QR code card for P421 Quick Start and P421User Guide.

About the P421

The P421 supports the Altowav AltoPlex Platform for 60 GHz wireless networks and provides wireless coverage for a 90° sector. See the D621 datasheet for specifications and features. See Design and Deployment for general design and deployment information, best practices and considerations based on network topology.

The RJ45 port and LED are located at the base of the unit.

The red/green LED on the bottom of the P421 device shows power, connection and activity.

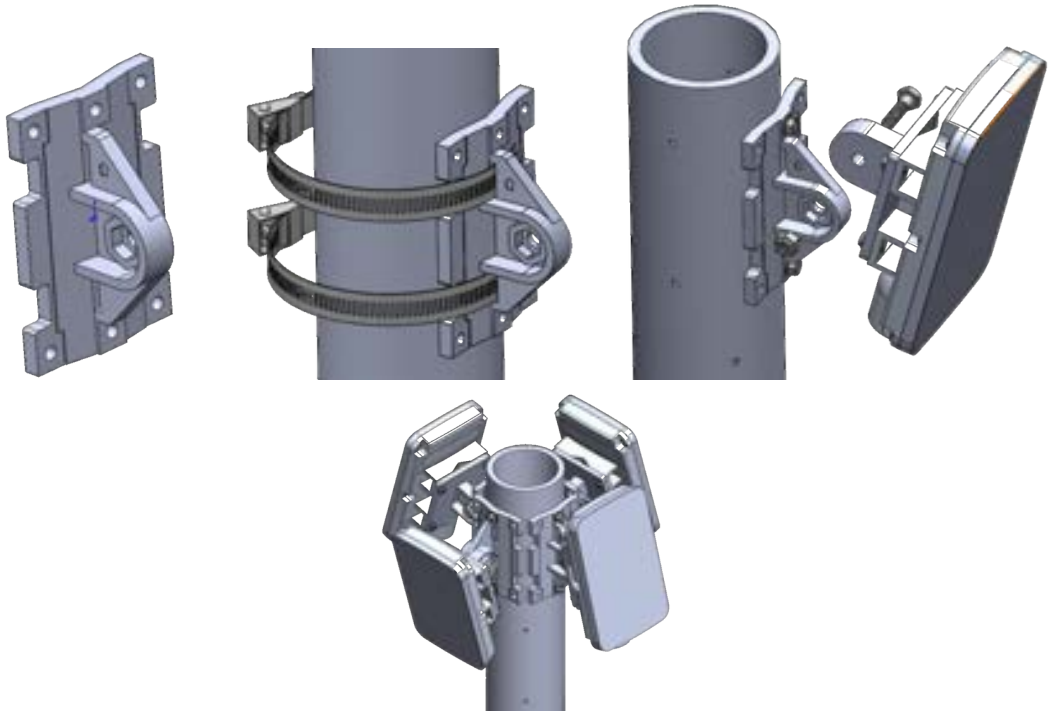
- Red — powering up.
- Flashing red and green — during boot up.
- Flashing green — until at least one wired link and one wireless link is formed.

- Steady green — normal operations with one or more wired and one or more wireless link.

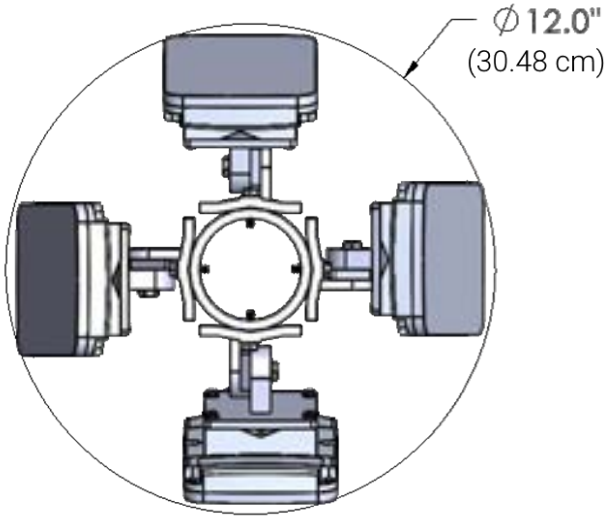
See LED Indicators for more detail.

Mounting options

Altowav model: AX-D6C4-MOUNT mounting brackets enable elevation adjustments from +60° to -45°. This model can be used for wall mount with screws, or pole mount with band clamps.



This equipment maintains a small form factor, even when installed for a 360° coverage.



PoE Injectors

Indoor and outdoor PoE Injectors are available.

		
30W Indoor PoE Injector **Model: AX-P-IN-AT-5G**	**Outdoor PoE switch** **Model: AX-PSW-OD-4AT-4C25**	**Mounting bracket** **Model: AX-PSW-OD-MOUNT**

Required network design information

Note: The terms DN and CN are used to describe the role of a device: distribution node or client node. Role determines how many wireless connections are possible. For example, many P421 devices operate in DN roles because they offer higher throughput, but can also operate as high throughput CNs. The role for a P421 can be configured on the Wireless tab of its WebUI. Specific model names are used when relevant.

Before installation the network design should be well planned and documented. A detailed network diagram for bench configuration and installation can help avoid costly, time-consuming adjustments after or during install. Required information for installation and configuration of the P421 in DN mode includes:

- The hostname and MAC address of the device, listed as **HN:** and **MA:** on the device label. Scan the QR code on the label for a text string that includes the MAC address.
- The planned wireless role (DN/CN), channel, Golay index and polarity for the P421.
- The MAC address for a **DN responder** - used to form a wireless link with another P421.
- The hostname of **CN responders** - used to configure a wireless link with client devices as they are installed. Note, **CN responders** should be added to the P421 configuration at the time they are installed, not before. The CN's host name is listed as **HN:** on the device label and included the QR code.
- The Management VLAN ID and PVIDs for this network site.
- Installation site information:
    - Planned azimuth for clear LOS between the devices on each end of each wireless link.
    - Any elevation changes for the install mount.
    - **Location/Description** information for configuration per your institution's requirements. Consistent information in these fields can be used by monitoring software, such as the AltoCommand, to identify specific devices in dense topologies.

This network diagram shows an example of how to communicate the required information for a ring topology. In this case there are no elevation differences noted.

> **Tip:** Adopt standard conventions and practices to help simplify design, installation and reading detailed network diagrams.

- **Boresight:** Position the P421 at an azimuth that makes DN links as close to boresight as possible.
- **Distance:** The shorter a link, the better the performance.

Prepare the PoE switch

The PoE switch must be prepared for installation. These instructions cover the preparation of the **Line AC** terminal and weatherproof installation of cable into the **PoE ports**. Examples of mounting the PoE switch are also provided.

Outdoor PoE switch **Model: AX-PSW-OD-4AT-4C25**	**Optional mounting bracket** **Model: AX-PSW-OD-MOUNT**
	

Note: LLDP is required for correct LAN peer identification for multiple P421 devices at one switch point. The AX-PSW-OD-4AT-4C25 switch supports LLDP. If using another switch, make sure it supports LLDP and that it is enabled.

1. **Prepare the outdoor PoE switch for AC power and mounting.**
    A. **Connect SO power cord (3-wire 18AWG) to the PSW AC Line terminal.**
        - **Estimate and cut the desired length of SO power cord.** Lengths will vary per conditions and equipment positions for each installation site. Be somewhat generous, extra can be trimmed when working at the site.
        - **Prepare wires for connection.** Unscrew the waterproof cap and gland from the **Line AC** port of the switch and slide it onto the SO cord as shown. Strip 25 mm (1 in.) of the cable jacket and 10 mm (3/8 - 1/2 in.) of insulation from each wire.

- **Replace each short wire in the AC Line terminal with the same color wire from the SO cord.** Unscrew and replace wires one at a time to ensure correct terminal connections — green to green, black to black, white to white.
- **Slide the waterproof gland and cap over the AC Line terminal and hand tighten each to the PoE switch housing**. The other end of the SO cord will be connected to AC power at the installation site.

2. **Connect the RJ45 end of cables to the Procet PoE ports.**
   A. **Remove the PoE end caps from the ports on the Procet.** Remove all components of the cable gland. Take note of the assembly order.
   B. **Cut a slit in each rubber grommet from top to bottom,** to allow inserting the Cat6 from the side when reassembling.

   C. **Reassemble the PoE switch end caps on the Cat6 and plug in the RJ45:**
      - Feed the RJ45 connector through the steel cap, then through the plastic grommet entering the splined end.
      - Slip the rubber grommet on the Cat6, using the slit made in the previous step. Position it between the plastic grommet and the RJ45 connector with the lip toward the RJ45.
      - Plug the RJ45 securely into the RJ45 slot inside a Procet PoE port. Listen for a click to verify a solid connection.
      - Slide all cable gland components up the Cat6 and into the PoE port. Components should self-align and seal adequately.
      - Fasten the steel end caps securely, but do not over tighten. The goal is tight enough to keep water out, without impacting the internal RJ45 connection.
      - Repeat the end cap reassembly for the remaining RJ45 connections.

Examples of outdoor PoE switch install:

- Metal pole mount with metal strapping and additional screws - not supplied.

- Wood pole with conduit mount - additional equipment: Pole mounting bracket AX-PSW-OD-MOUNT, conduit, conduit straps, and strut channel.

Installation at Network Site

Installation tips:

- Install the P421 on the pole or wall with no obstructions above the unit to enable the GPS synchronization.
- Maintain **clear line of sight (LOS)** at the front of the P421 for links. Best performance is achieved with boresight alignment between P421 wireless devices, so this is recommended for DN-DN links.
- **Power source:** For outdoor use, the 4 Port 2.5G PoE switch (Altowav Model AX-PSW-OD-4AT-4C25) is recommended. The outdoor PoE switch can provide power for up to four connected devices. If weatherproof enclosure is available on site and power for only one device is required, the AX-P-IN-AT-5G (30 W indoor PoE injector) can be used.

  If a customer-supplied switch is used: Make sure the switch supports LLDP and that it is enabled. Also be aware that managed switches with RSTP enabled increase the hop count for RSTP.
- When adjustments to positioning or aiming the P421 are done after the device is linked to other devices, power cycle the unit. To power cycle, simply disconnect the device from power and reconnect it.

At the installation site:

Note: A clear line of sight must be maintained for an optimal wireless link, preferably at boresight for DN links.

1. Install the ground wire, if required by code, at the installation location. Connect the other end of the ground wire to nearby good earth.

2. Install an outdoor-rated Cat6 cable in the port on the P421 device:

A. Unscrew and deconstruct the components of the gland.

B. Insert the Cat6 cable in the gland as shown.

C. Secure the components of the gland and attach the Cat6 cable to the device's RJ45 port and attach the gland to the device. Do not overtighten.

3. Mount the device to a wall or pole at the installation location with the mounting bracket (see Mounting options). Ensure a clear line of sight to the connecting distribution node.

4. Connect the other end of the Cat6 cable to the PoE port on the PoE injector. Connect the PoE injector to AC power. **Note,** the supplied PoE injector is an indoor unit so it requires a weatherproof box for outdoor installation.

5. Verify that the device powers up. (LED is red during boot-up and then flashing green.)

6. **Mount the first P421 on the pole or wall, with no obstructions to wireless link LOS or obstructions to GPS above the unit.** Make sure the P421 is oriented according to the planned azimuth and elevation for clear LOS to the device at the remote end of the wireless link.

   Make sure the install location has no obstructions above the unit for clear GPS operation.

7. **Install other P421s at the same site using the previous steps, according to the design plan.** Devices connected through a PoE switch at the same site will become LAN peers via their wired connection through the PoE switch.
8. **Move to the next site and mount the P421 that will link to the first P421.**
   A. Mount the connecting device.
   B. Power up.
   C. Perform DN link auto-configuration.

      Note: If DN link auto-configuration isn't used, all devices should be bench configured prior to mounting the devices.

9. **For multi-link backhaul or ring topologies, install the remaining P421 devices according to the detailed network plan.**
   A. **Work outward from the PoP**, for ring and multi-link backhaul topologies.
   B. **Retest distribution ring or multi-link backhaul to verify wireless and LAN peer connections, when all P421 devices are installed and powered up.** Ensure that each P421 is found and review its performance, adjust and fine tune before finalizing the installation and adding clients.

      Note: If the P421 is repositioned or re-aimed after DN connections are made, rebeamform the link by resetting the **DN responder** on one end of the link,

rebooting, or power cycling the unit. Resetting the responder is the least disruptive method to an operational network.

C. **Verify through the WebUI** that each P421 is connected per the network design. This sample of the Wireless table on the Status tab shows a P421 connected to another P421 (KB-C0-00-01).

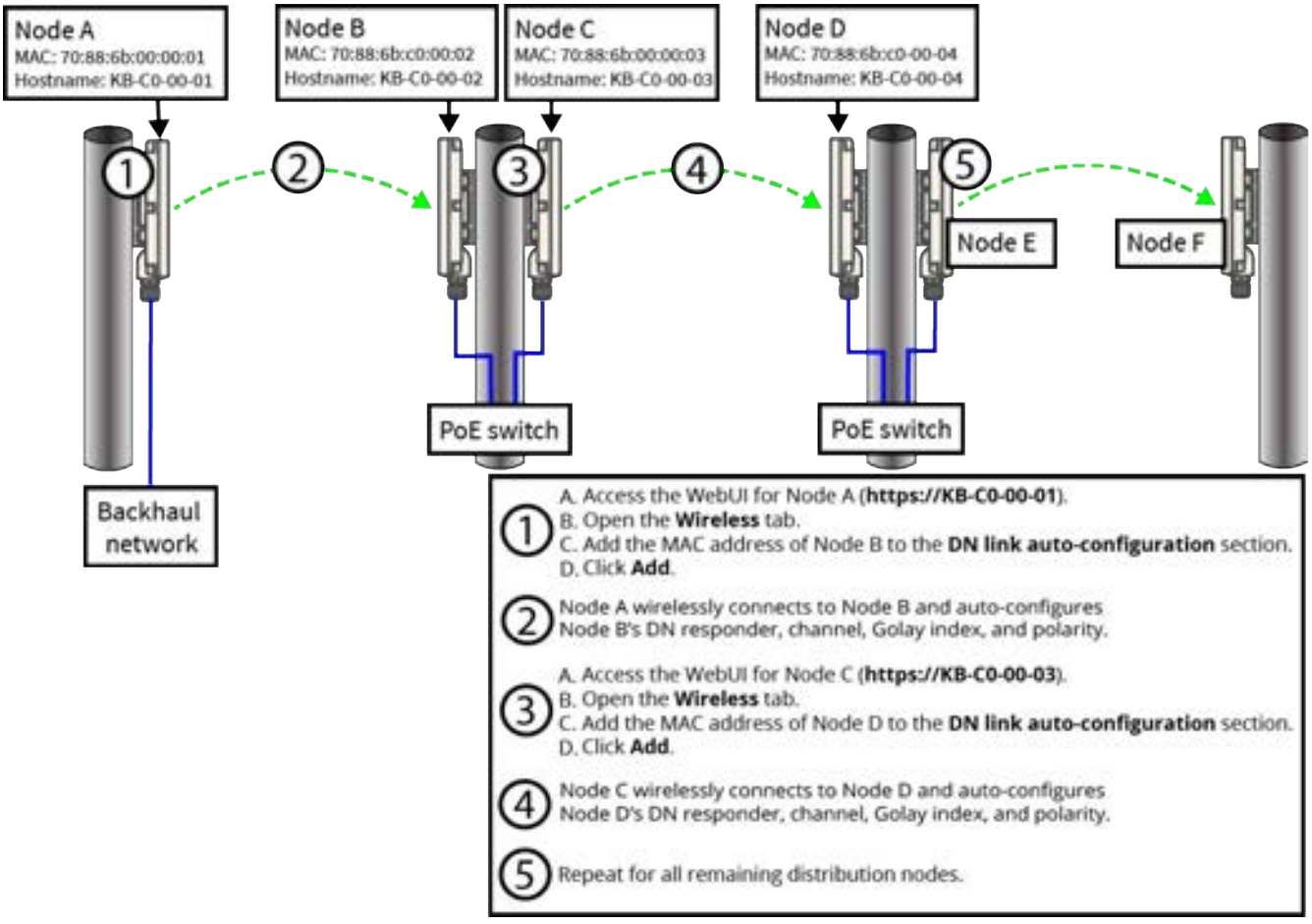
D. **Check signal quality.** For example, a P421-P421 link should have an RSSI of greater than -65. Expected MCS for a P421-P421 link is 9 for up to 250 m, and 12 for up to 150 m with significant traffic.

DN link auto-configuration

When devices are installed based on your network design, you can use the DN link auto-configuration feature to automatically configure wireless links between distribution nodes.

Prerequisites:

- During physical installation, the installer should note the MAC address and hostname of each device, along with the location and direction that the device is facing.
- The hostname and MAC address of the device are listed as **HN:** and **MA:** on the device label and contained in the QR code on the label, as shown in Required network design information.
- DHCP should be enabled on the backhaul network.

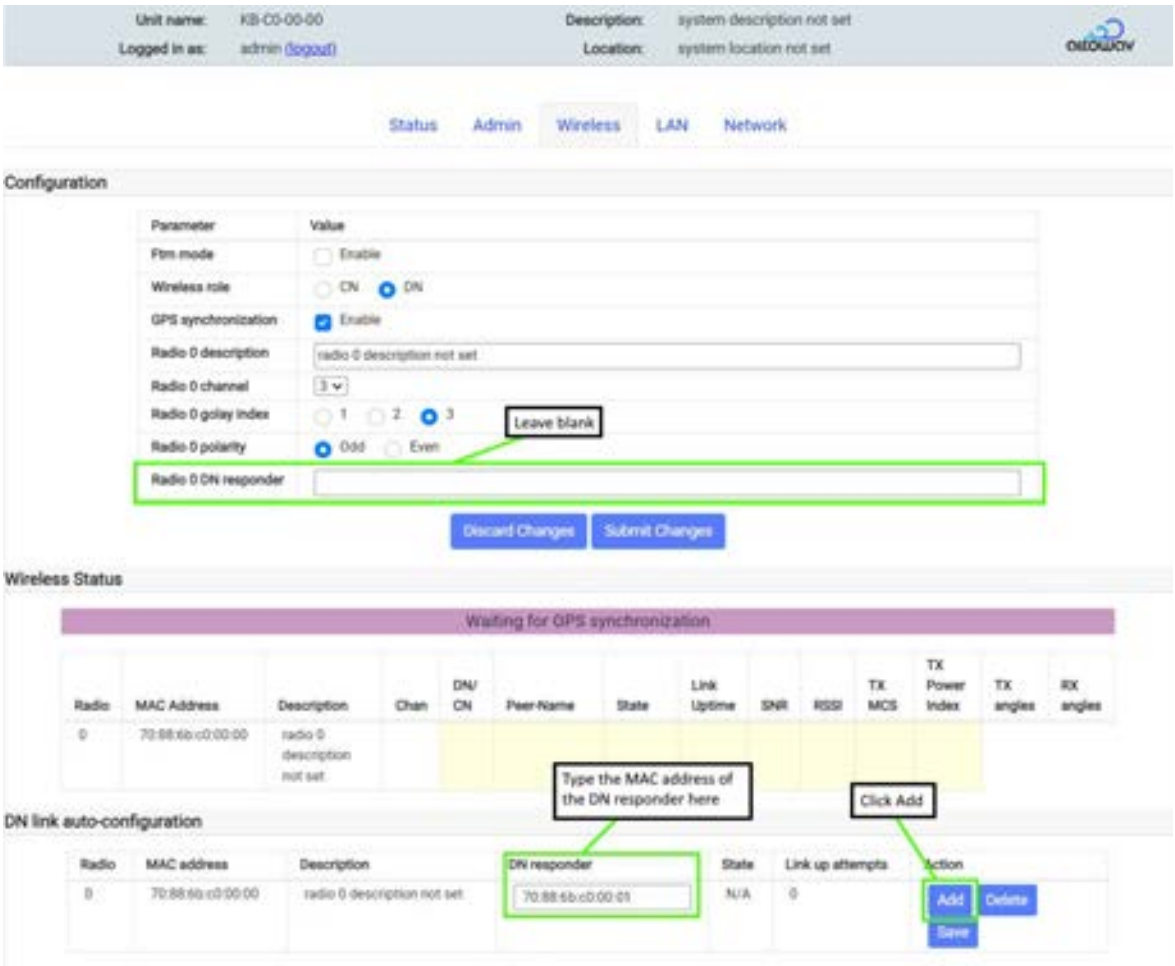


DN link auto-configuration process flowchart

To auto-configure DN links:

1. Connect the first DN initiator node to the backhaul network and log into the WebUI for node by typing **https://<hostname>/** into a browser address bar from a PC connected to the network, or connected to the device by its Wi-Fi Connection.
   A. Click the **login** link in the WebUI header to log in as administrator. The username is **admin**, and the default password is **admin**.

   B. On the **Wireless** tab, in the **Configuration** section, leave the **DN responder** field blank.
   C. In the **DN link auto-configuration** section, type the MAC address of the **DN responder**.
   D. Click **Add**.



   E. Perform other configuration as desired. See Configuration via the WebUI.
2. Once the airlink between the DN initiator and DN responder is established, the responder will be automatically configured to include:

- The MAC address of the initiator for the **DN responder**.
- The **channel** and **Golay index** being used by the initiator.
- The opposite **polarity** of the initiator.

3. Log into the next DN initiator node.
   - If DHCP is enabled and the next DN initiator is connected via a switch to the DN responder configured in step 2 (as shown in the process flowchart, above), the hostname of the next DN initiator should be resolvable and you can type **https://<hostname>/** into a browser address bar.
   - If the hostname of the next DN initiator is not resolvable, do one of the following to determine its IP address:
     - Use the `ll_discovery` REST API to determine the device's IP address:

       In a browser, type:

       `https://<hostname>/rest/v002/device/ll_discovery`

       where *hostname* is the hostname or IP address of the DN responder configured in step 2.

       Using `ll_discovery` requires that the switch is configured to forward LLDP.

     - Use the `kb_browse ex` command:
       1. ssh into the DN responder configured in step 2.
       2. At the command prompt, type `kb_browse ex`:

```
KB-C0-00-02> kb_browse ex
=    br0 IPv4 KB-C0-00-03
 _kwikbit._tcp        local
   hostname = [KB-C0-00-03.local]
   address = [10.0.0.01]
   port = [443]
   txt = ["description="system description not set""
"location="system location not set""]
```

          This command returns information about all AltoPlex devices connected to the node, including the hostname and IP address.

   A. On the **Wireless** tab, in the **Configuration** section, leave the **DN responder** field blank.
   B. In the **DN link auto-configuration** section, type the MAC address of the **DN responder**.
   C. Click **Add**.
   D. Perform other configuration as desired. See Configuration via WebUI.
4. Once the airlink is established, the DN responder will be auto-configured as described in step 2.
5. Continue this process for all of the distribution nodes in your system.

Optional bench configuration

As an alternate to performing DN link auto-configuration, you can configure the devices prior to installation, a process referred to as bench configuration.

Summary of bench configuration settings:

- Admin tab:
  - **Location** — Recommended.
  - **Description** — Recommended.
  - **Upgrade Firmware** — As needed.
- **Wireless** tab, **Configuration** section:
  - **Wireless role** — Defaults to **DN**.
  - **DN responder** — Required to form DN-DN links.
  - **Channel**, **Golay**, **Polarity** — Required per design.
- LAN tab: Review to ensure Port 1 is enabled (default).
- Network tab: Review
  - **IP Addressing mode** — Defaults to **Dynamic**.
  - **VLAN configuration** — Defaults to working values for installation out of the box. After installation is verified, update the VLAN configuration as required for your design.
  - **Spanning Tree Protocol**, **SNMP**, **Network Services**, and **DHCP Relay** configuration — Recommended, per your network.

Configuration via the WebUI

The P421 can be configured through the WebUI. Access the WebUI by using one of the following methods:

- Access the WebUI by typing the hostname or IP address of the P421 (**https://<hostname>/**) into a browser address bar from a PC connected to the network.
- Link from the Wireless table of a connected device's WebUI by clicking the name of the device to configure in the **Peer Name** column of that table.

- If using the AltoCommand, access the WebUI from the **Devices** page by clicking at the end of a device's row and clicking **Connect to Device**.

Some common tasks at the WebUI:

- View information about the device, its firmware version, its wireless connections, its LAN interfaces, and Management interface on the **Status** tab. You can also click on a **Peer-Name** to access the WebUI for a connected device.
- Click on the **Admin** tab and do one of the following: **Upgrade Firmware**, **Change Password**, **Locate the Unit**, **Download a Diagnostic File**, **Reboot**, **Restore Factory Defaults**, set **Location** or **Description** per your network design plan, or configure **Diagnostic Wi-Fi settings**.
- Click on **Wireless** tab. If DN link auto-configuration is used, the **DN responder** (MAC address for a connecting P421 device), **Channel**, **Golay index**, and **Polarity** will be automatically configured.

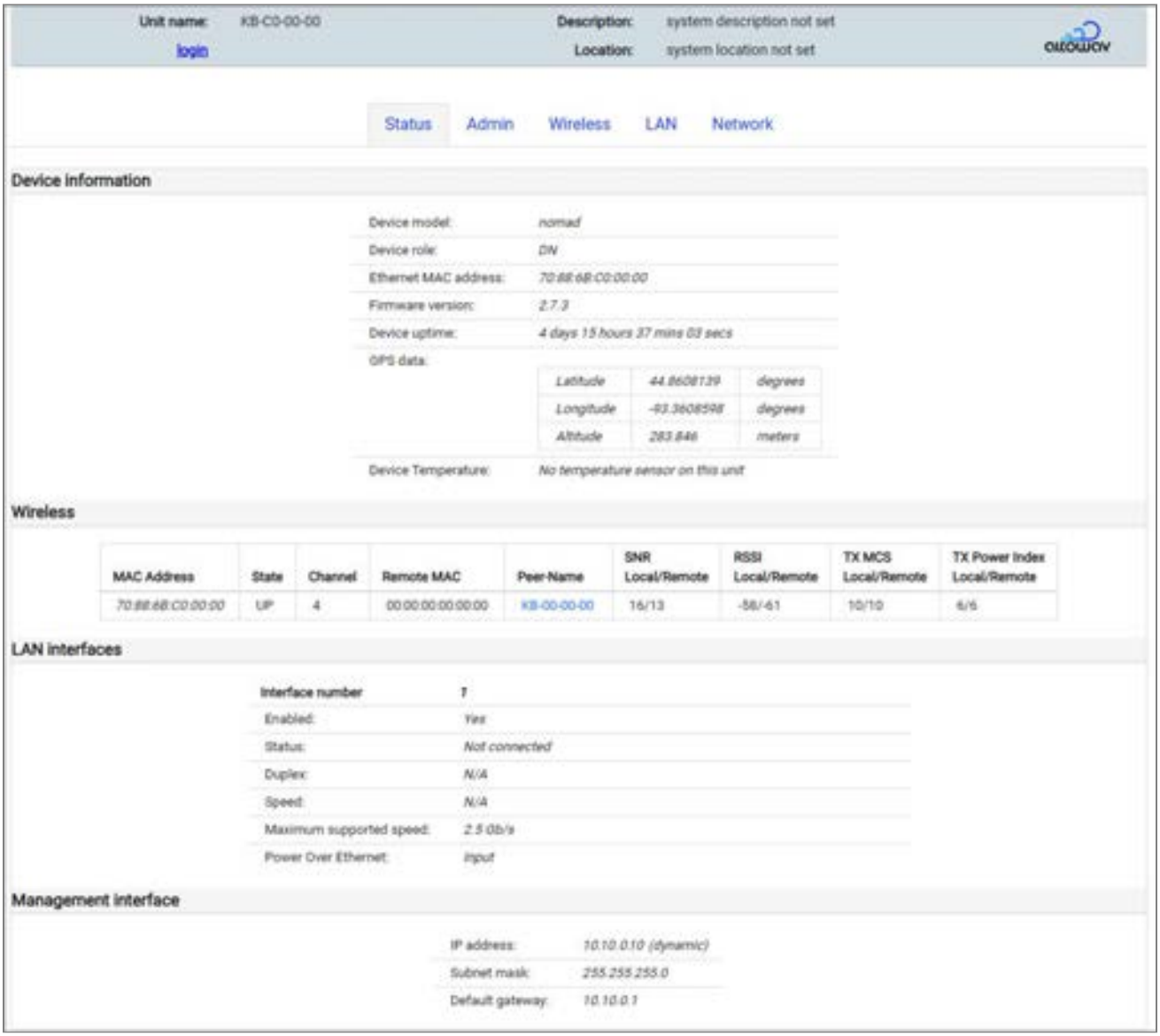
  Note: If DN link auto-configuration is not used, you should set the **DN responder**, **Channel**, **Golay index**, and **Polarity** as part of bench configuration prior to the devices being installed.
- On the **Network** tab, set network configuration items for Management, VLAN.

The header of the WebUI shows the **Unit name** of the P421 (also called the hostname), **Description** and **Location**, as well as offering a **login** link.

Tip: The header background changes from gray to yellow when a unit is unreachable.

Status tab

The **Status** tab shows a summary of information about the unit, its wireless and LAN connections, and interface information.



Status tab — Device Information section

This section shows the model name, MAC address, firmware version, device uptime, GPS data, and device temperature.

> **Tip:** The **Status** tab shows the current firmware version. Firmware can be updated using the **Upgrade Firmware** button on the **Admin** tab. It is generally recommended that all devices in the network use the same firmware version.

Status tab — Wireless section

The table in this area shows wireless link status for the unit. Use the horizontal scroll bar to view all values. Information includes Radio, MAC Address, Description, Channel (1-4), the role of the peer listed (DN), Peer-Name, State (UP or DOWN), SNR, RSSI, TX MCS, TX Power Index, TX angles and RX angles. Tip for DN device tables, hover over a column heading for a description of the values.

Values for **SNR, RSSI**, **TX MCS** and **TX Power Index** show values for both ends of the link – local/remote.

> **Tip:** To access the WebUI for a peer, click on the name listed under Peer-Name. A new browser tab opens for the named device's WebUI.

Status tab — LAN interfaces section

This area shows information for the LAN interface, (Port 1 for the P421) including whether the port is enabled, its Status (Connected or Not connected), Duplex mode, Speed, Maximum supported speed, and PoE mode.

Status tab — Management interface section

This area lists the MGMT interface IP address, Subnet mask and Default gateway. It also shows how the IP was assigned (dynamic or static.)

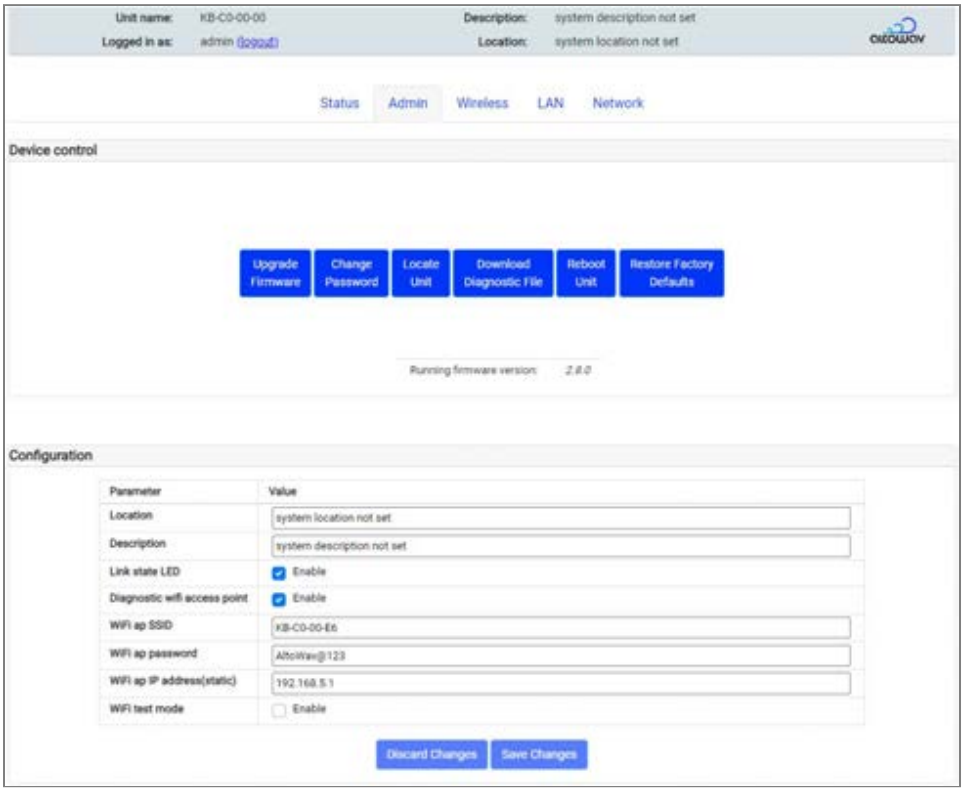
Admin tab

Unauthenticated users can view read-only information about the device in the WebUI. To make changes to the configuration, you must be logged in as an administrator.

Click the **login** link in the WebUI header to log in as administrator. The username is **admin**, and the default password is **admin**.

During initial configuration, enter a location and description for the node, and if required, change the password.

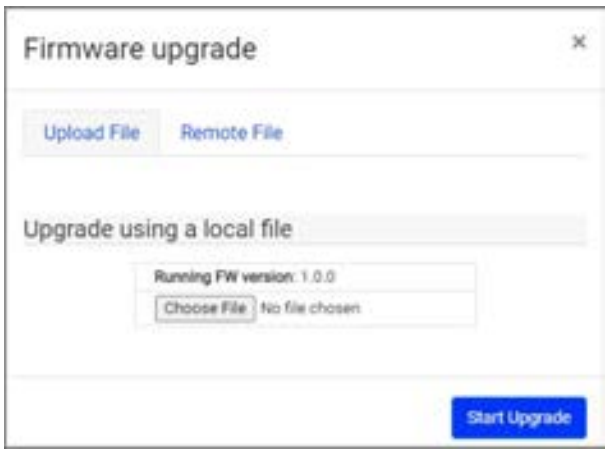
Other options available include **Upgrade Firmware**, **Locate Unit**, **Download Diagnostic File**, **Reboot Unit**, and **Restore Factory Defaults**.



Admin tab — Device control section

This section lists the firmware version on this device. This area also offers buttons for the following tasks:

Upgrade Firmware — updates the device firmware with the file you choose. Click the **Upgrade Firmware** button and upload or browse to the firmware upgrade file. Then click **Start Upgrade**. The device will reboot as part of the upgrade process. For more detailed steps see the Upgrade Firmware topic.



> **Tip:** The AltoCommand management interface also offers a convenient way to review firmware version compliance for all AltoPlex devices in your network, and upgrade them from the Devices list.

Change Password — Use this button to change the password for the admin of the P421.

Locate Unit — Click this button to put the unit into locate mode. In locate mode, the device flashes an LED signal for field personnel to identify the unit. LED sequence: LED flashes, alternating red and green.

Download Diagnostic File — Automatically downloads a detailed diagnostic text file for the device. The file contains detailed information about the device and its status at the time of the download. The file name includes the hostname, the date and time. For example, a file named KB-C0-01-01_diag_2024-10-09-14-43-32.txt, means this is the diagnostic text file for the device KB-C0-01-01, created at 2:43:32 pm (UTC) on October 09, 2024.

Reboot Unit — Restarts the unit remotely.

Restore Factory Defaults — Restores all device configuration to factory defaults. If the unit is unreachable and cannot be reset with this button, it may require a hard factory reset. See the Factory Reset topic for instructions

Note: Factory reset returns the unit's password to the default: **admin**. Since the IP assignment uses DHCP by default, the factory reset is not likely to affect the IP address of the device.

Admin tab — Configuration section

This section includes the following settings:

Location — Indicates the physical location where the device will be installed.

Description — May include orientation, function, role or other information about the device. The AltoCommand web-based management tool can automatically use this field as a Switch point tag, when populating the network map , so similar but unique descriptions are recommended.

Link state LED — Enables or disables the LED for displaying the node status. See LED indicators.

Diagnostic wifi access point — Enables / disables Wi-Fi access for the unit. Default: **Enable**. See Wi-Fi Connection to a D621 or P621 for when and how to use the Diagnostic Wi-Fi access point.

Note: Disabling this setting turns off the Wi-Fi access point completely, (not just the Wi-Fi user interface). The device will not be seen by a Wi-Fi search when this setting is disabled.

WiFi ap SSID — Sets the SSID for the diagnostic Wi-Fi access. The SSID defaults to the device's Host Name (KB-XX-XX-XX).

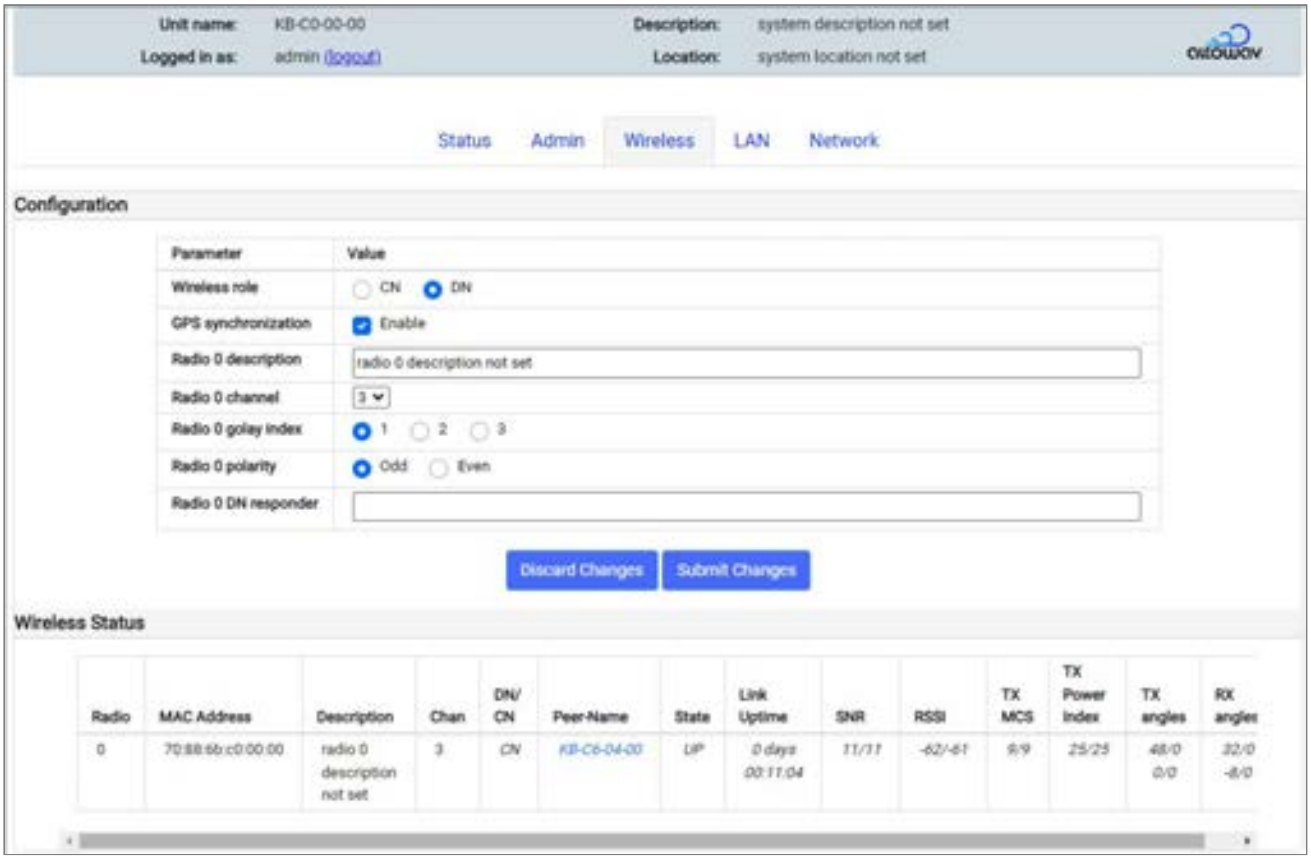
WiFi ap password — Sets the password for the diagnostic Wi-Fi access. Default setting: AltoWav@123.

WiFi ap IP address (static) — Sets a static IP address for diagnostic Wi-Fi access. Default setting: 192.168.5.1.

Wireless tab

The Wireless tab includes configuration of the device's wireless role, a GPS synchronization checkbox, radio description, channel, Golay index, polarity, and DN responder. The Wireless status table is also included on this tab, enabling you to view the state of RF links, verify connections and browse to peers, as needed.

> **Tip:** After clicking **Submit Changes**, stay on this tab until the links reset and the Wireless status table updates. This ensures that settings and links are complete before more changes are made.



Wireless tab — Configuration section

The following configuration settings are used to make the device's links unique, in order to form and secure a wireless connection with another device and to avoid co-channel interference.

Wireless role — The P421 can only serve in a DN (distribution node) role.

GPS synchronization — Enables or disables GPS synchronization. The P421 uses GPS for location and TDMA synchronization. When GPS Synchronization is enabled or disabled, the device will reboot once the change is submitted.

Description — Enter a meaningful description to assist field technicians during installation or troubleshooting. For example, "Pole 37, aimed toward KB-C6-xx-xx".

Channel set the channel frequency, 1-4.

Channel	Center (GHz)	Min. (GHz)	Max. (GHz)
1	58.32	57.24	59.40
2	60.48	59.40	61.56
3	62.64	61.56	63.72
4	64.80	63.72	65.88

Golay index set the Golay index, 1-3. Golay index can be useful for avoiding certain types of co-channel interference. See the D621 Design and Deployment topic.

Polarity set polarity to odd or even.

DN responder is automatically set if DN link auto-configuration is used. The represents the MAC address for the wireless interface to a remote distribution node. Only one DN responder link is allowed.

The **Submit Changes** button resets the link configuration to the values selected. Link configuration changes are shown in the Wireless Status table as they become complete.

Note: Enable/disable **GPS Synchronization** causes a reboot of the device.

Wireless tab — Wireless section

The wireless status table is the same information shown in the Wireless table on the Status tab.

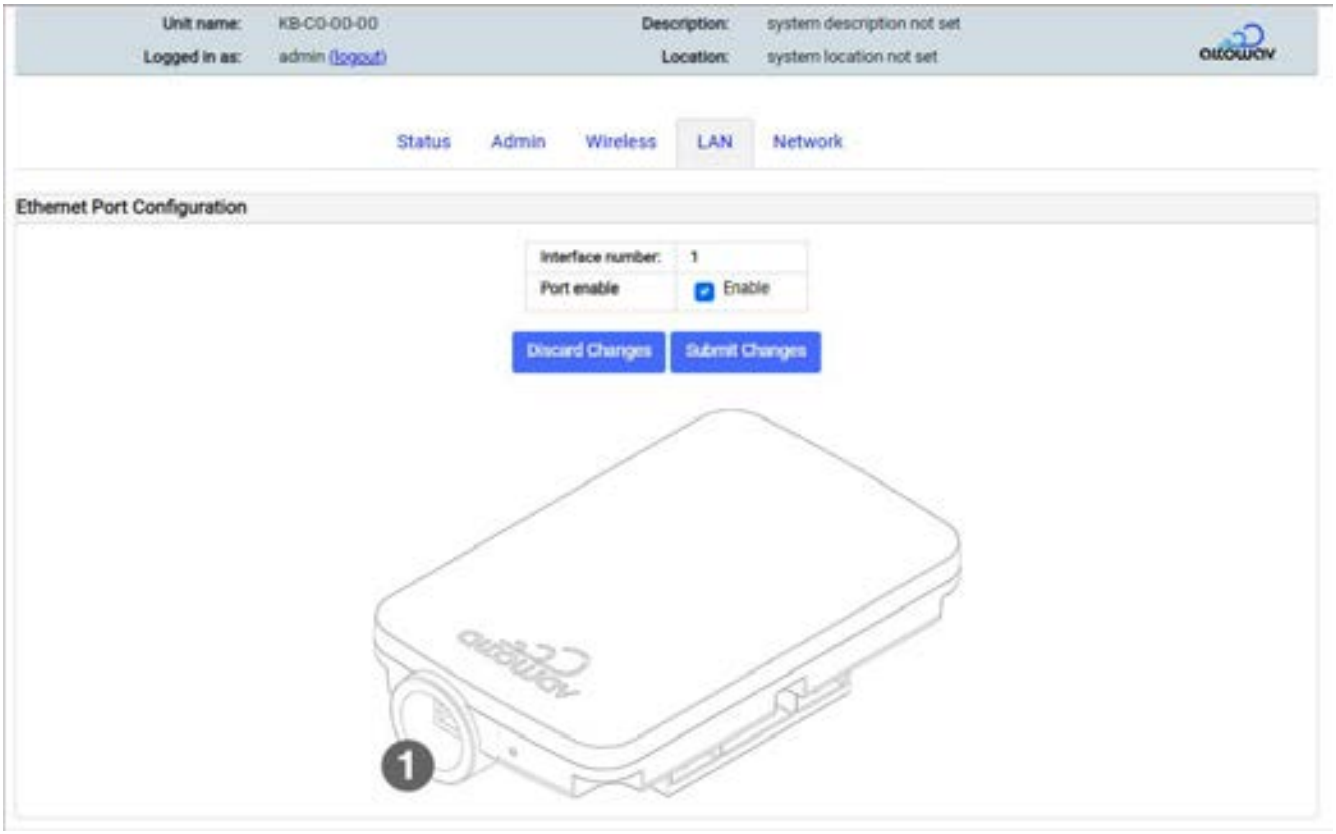
The table in this area shows wireless link status for the unit. Use the horizontal scroll bar to view all values. Information includes Radio, MAC Address, Description, Channel (1-4), the role of the peer listed (DN), Peer-Name, State (UP or DOWN), SNR, RSSI, TX MCS, TX Power Index, TX angles and RX angles. Tip for DN device tables, hover over a column heading for a description of the values.

Values for **SNR, RSSI**, **TX MCS** and **TX Power Index** show values for both ends of the link – local/remote.

> **Tip:** To access the WebUI for a peer, click on the name listed under Peer-Name. A new browser tab opens for the named device's WebUI.

LAN tab

The LAN tab provides settings for enabling Ethernet traffic on the LAN port for the P421.



Ethernet Port Configuration

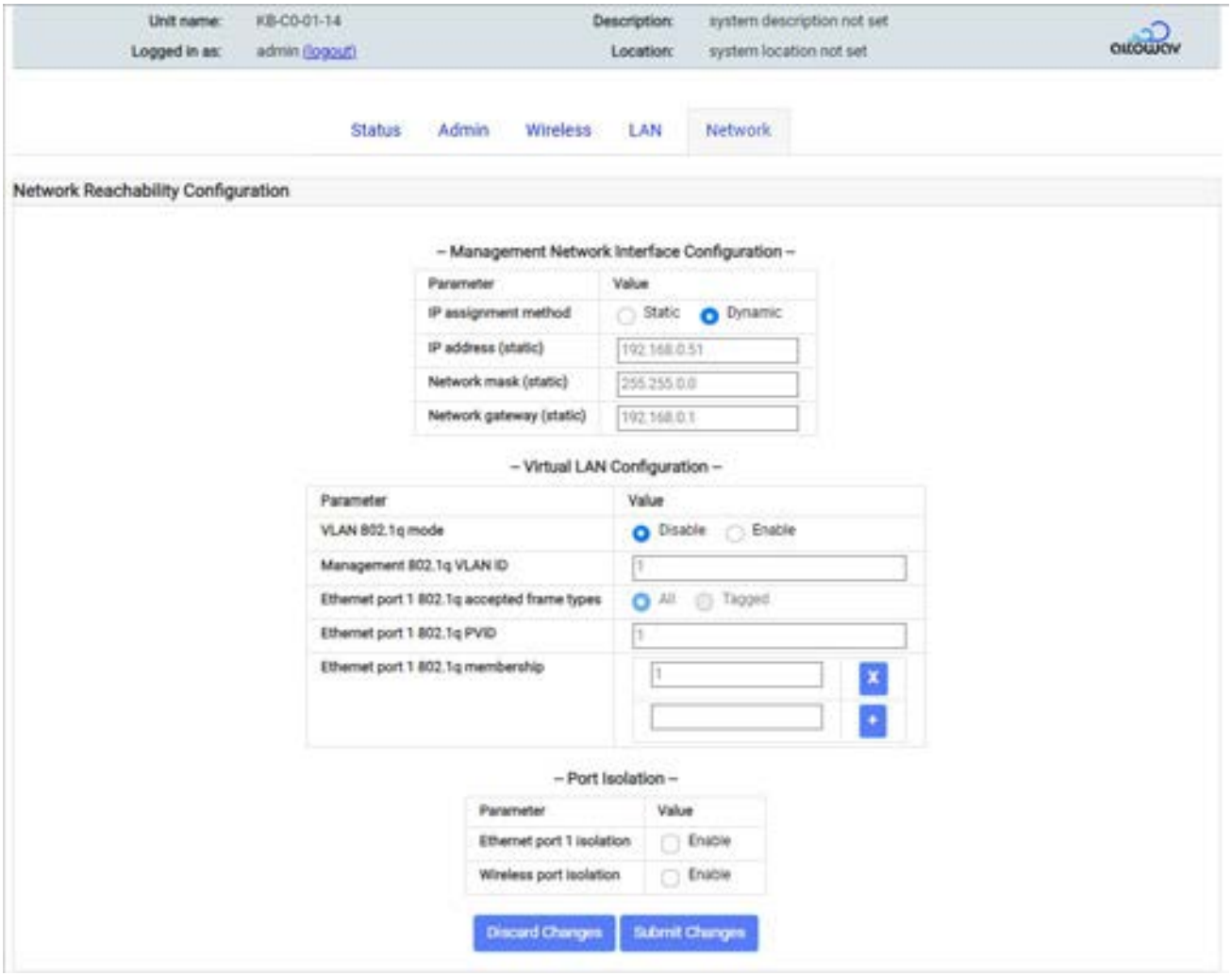
Port enable — Check or clear the box to enable/disable the Ethernet port traffic. The PoE input remains active.

The port is enabled by default.

> **Tip:** In the WebUI, hover over the port in the graphic to show the current connection status of the port.

Network tab

The top half of the **Network** tab contains Network Reachability Configuration settings. They include settings for Management Network Interfaces, VLAN Configuration and Port Isolation.



Network tab — Network Reachability Configuration section

Note: With AltoPlex technology, a P421 operating in a Distribution Node role establishes a wireless link with a device in a client node role when that client is installed and added to the **CN responder** list. Once connected, the clients remain reachable for management traffic regardless of VLAN settings. This operation eliminates a problem seen with Gen2 (802.11ad) technology where incorrect VLAN settings could render a device unreachable via airlink.

Management Network Interface Configuration — IP assignment method defaults to **Dynamic**. If set to **Static**, it also requires an **IP address**, **Network mask** and **Network gateway**.

Virtual LAN Configuration — These settings use IDs to control data communication between nodes. VLANs can be used to create segments within a larger network, limiting access to the VLAN to a specific set of users. The settings used to support the creation and use of VLANS include 802.1q mode and management VLAN ID, setting accepted frame types (all or tagged) and a PVID for the Ethernet port.

Port Isolation — This can be enabled to restrict traffic between nodes in the VLAN.

Network tab — Additional Layer 2 Settings

Spanning tree protocol — Enable/disable spanning tree protocol (STP) by checking/clearing the box. If enabled, optionally set the bridge priority and port path cost for the wireless interface.

Bridge priority is used to determine which device will serve as the root of the STP bridge. The device with the lowest priority will serve as the root. The priority configured here is a multiplier; to determine the actual STP priority, multiply by 4096.

The **port path cost** is used to determine the preferred path to the root. The path with the lowest cumulative cost is used.

Network tab — SNMP Configuration

Settings in this section enable the SNMP agent for monitoring and reporting events on the nodes in your network. Other settings configure how and to whom the SNMP messages are sent.

Network tab — Network Services Configuration

This section sets a **DNS IP list** and the selection of an **NTP server**.

DNS IP address lists are entered in dotted decimal format, using commas to separate the IP addresses.

Note: The **NTP server** field is only enabled when a **DN** role is selected for the device and **GPS Synchronization** is disabled (on the Wireless tab of the WebUI). NTP servers may be useful during bench configuration or testing in indoor locations where GPS is not available.

DHCP Relay Configuration (Option 82)

Use these settings to enhance security for DHCP assignment of IP addresses. Enable the DHCP relay agent and select its circuit ID type (**HWaddr** or **Hostif**).

Select whether to enable access for only **Trusted** sources or **Untrusted** (any) source.

Maintenance and security

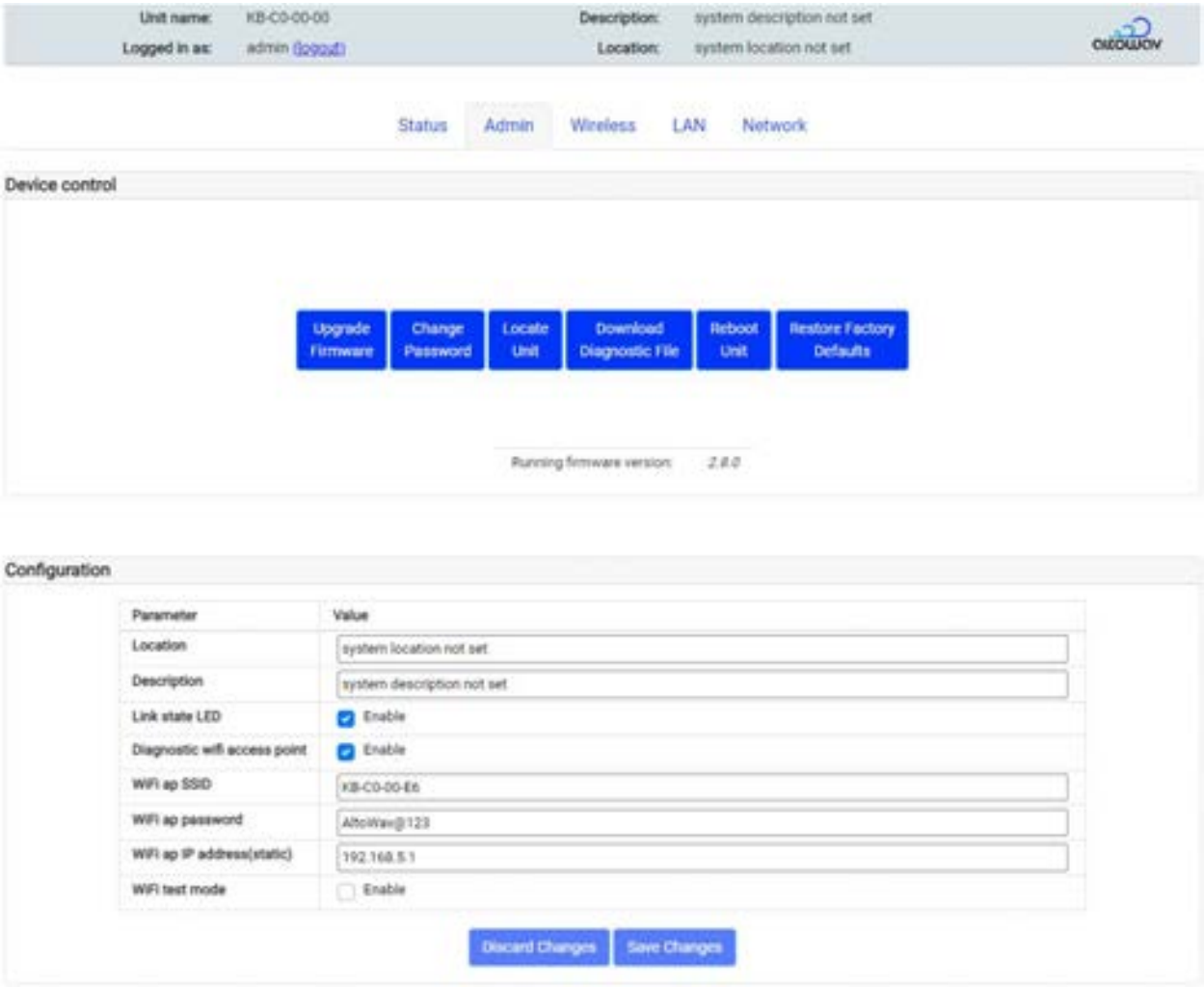
Change a device password

For all AltoPlex devices, passwords can be changed using the WebUI. The process is the same for all devices.

Note: Take care when changing passwords, so the device's WebUI is not rendered unreachable.

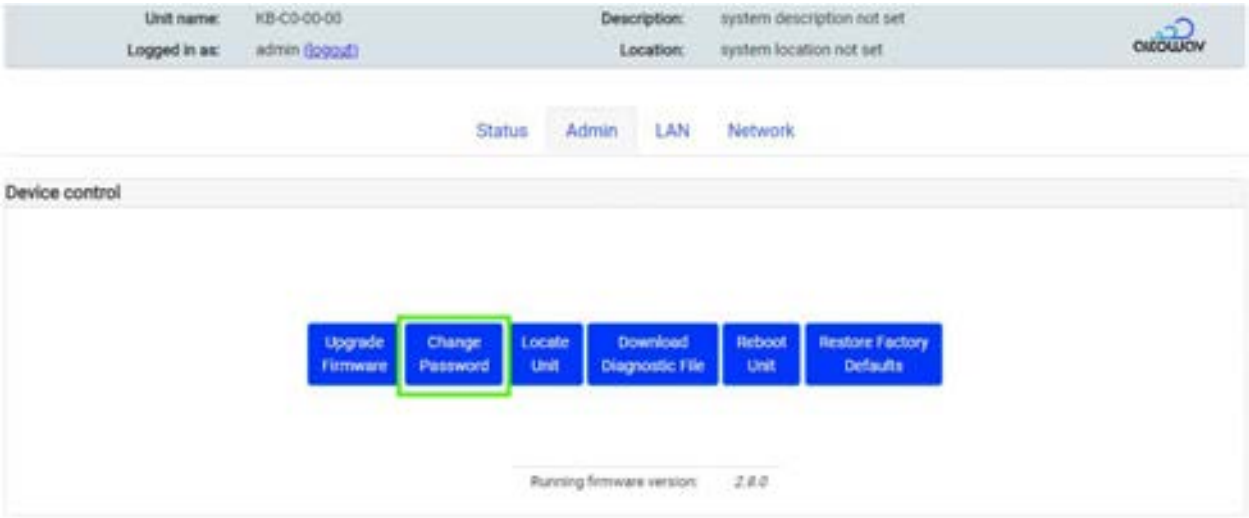
To change the device password:

1. In the WebUI, click the **Admin** tab.



2. Click the **login** link in the WebUI header to log in as administrator. The username is **admin**, and the default password is **admin**.

3. Click the **Change Password** button in the Device control section.



The **Change user password** dialog opens.

4. Enter and re-enter the new password and click **Change Password**.

Enable Passwordless SSH

By default, the P421 requires a password to log onto the device when using SSH. You can use the **ssh_keys** CLI command to configure passwordless SSH login to the P421.

1. Generate SSH keys on your local device.
2. log in via ssh to the P421:

   ```
   $ ssh admin@<hostname>
   admin@<hostname>'s password:
   ```

   where *hostname* is the hostname (for example. KB-C0-01-01) or IP address of the device.
3. Enter **control** mode:

   ```
   KB-C0-01-01> control
   KB-C0-01-01(control)>
   ```
4. Use the **ssh_keys** command:
   - Use **ssh_keys add file *user@host:/path*** to add a key that is stored on a different host, where:
     - *user* is the username to log into the host.
     - *host* is the name of the host machine.
     - *path* is the path and filename of the key file.
   - Use **ssh_keys add text *key*** to add a key by copying the contents of the key file and pasting the contents as an argument of the **ssh_keys add** command.
   - Use **ssh_keys show** to return a list of installed keys.
   - Use **ssh_keys delete *number*** to uninstall the key specified by *number*. The number of the key is determined with the **ssh_keys show** command.
   - Use **ssh_keys delete all** to uninstall all keys.

Note: All authorized keys are deleted when a factory reset is performed.

Upgrade firmware

Upgrade roadmap

Note: The role of the device (distribution node (DN) or client node (CN)) affects the sequence of upgrading.

1. Download the new firmware version from Altowav Altoplex Firmware Downloads at support.altowav.com.
2. Upgrade the devices one at a time.
3. Always start with the distribution node unit furthest from the root node.
4. Make sure each upgrade finishes and all DN and CN links are re-established before moving on to the next distribution node.

> **Tip:** When upgrading a distribution node, make note of any connected client nodes that are offline at the time of the firmware upgrade. Before running the upgrade, remove them from the **CN responder** list for the distribution node. After the upgrade completes, the client nodes can be added back into the distribution node configuration. This process ensures that a distribution node will not try to reconnect to a client node which is known to be offline.

Preliminary steps for using TFTP with the WebUI or CLI Method

When using a TFTP server for upgrades via the WebUI or CLI, complete these steps:

1. Download and unzip the upgrade files from Altowav Altoplex Firmware Downloads at support.altowav.com.

   The following files are included in the zip file:

   - A digest file
   - The firmware file

   The firmware filename consists of three parts:

   <product_name>-<device_family_name>-<version_number>

   where:

   - *product_name* is **kb_sw-prod**
   - *device_family_name* is one of:
     - **NOMAD** — Firmware used for D621 and P621 devices.
     - **DEVO** — Firmware used for C410, C420, and P421 devices.
   - *version_number* is the version number of the firmware.

For example:

kb_sw-prod-DEVO-2.8.0

2. Rename the digest file to **kb_sw_image_digest** and view the renamed file to verify that its contents match the name of the downloaded software version.
3. Upload the files to the TFTP directory on your server. The TFTP server must be accessible from each device being upgraded.

Upgrade from the WebUI

Upgrade from a local file

To upgrade from a local file by using the WebUI:

1. Download and unzip the upgrade files from Altowav Altoplex Firmware Downloads at support.altowav.com.

   The following files are included in the zip file:

   - A digest file
   - The firmware file

   The firmware filename consists of three parts:

   <product_name>-<device_family_name>-<version_number>

   where:

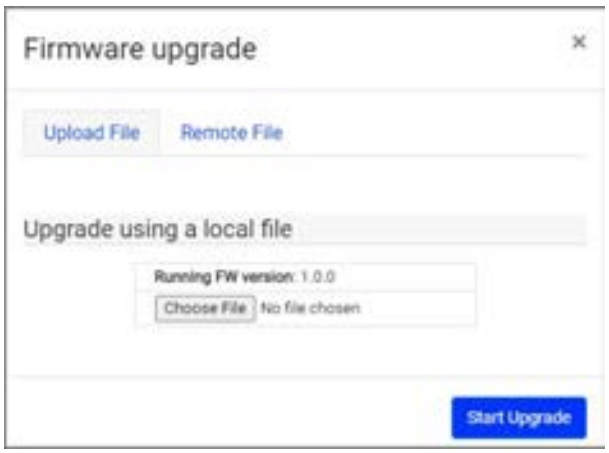
   - *product_name* is **kb_sw-prod**
   - *device_family_name* is one of:
     - **NOMAD** — Firmware used for D621 and P621 devices.
     - **DEVO** — Firmware used for C410, C420, and P421 devices.
   - *version_number* is the version number of the firmware.

   For example:

   kb_sw-prod-DEVO-2.8.0

2. Open the WebUI of the device to be upgraded and click the **Admin** tab.
3. Click the **login** link in the WebUI header to log in as administrator. The username is **admin**, and the default password is **admin**.

4. Click the **Upgrade Firmware** button.
5. Click **Choose File**.
6. Browse to the directory where the upgrade file was downloaded and select the file.
7. Click **Start Upgrade**.



Upgrade from a TFTP server

1. Download and unzip the upgrade files from Altowav Altoplex Firmware Downloads at support.altowav.com.

   The following files are included in the zip file:

   - A digest file
   - The firmware file

   The firmware filename consists of three parts:

   <product_name>-<device_family_name>-<version_number>

   where:

   - *product_name* is **kb_sw-prod**
   - *device_family_name* is one of:
     - **NOMAD** — Firmware used for D621 and P621 devices.
     - **DEVO** — Firmware used for C410, C420, and P421 devices.
   - *version_number* is the version number of the firmware.

   For example:

   kb_sw-prod-DEVO-2.8.0
2. Open the WebUI of the device to be upgraded and click the **Admin** tab.
3. Click the **login** link in the WebUI header to log in as administrator. The username is **admin**, and the default password is **admin**.

4. Click the **Upgrade Firmware** button.

5. Click the **Remote File** tab.
6. For **TFTP server**, type the URL of the TFTP server.
7. Click **Check for Newer Firmware**.

   A message will indicate if the firmware on the TFTP server is newer than the firmware on the device.
8. If newer firmware is found, click **Start Upgrade**.

Upgrade from the CLI

1. log in via ssh to the P421:

   ```
   $ ssh admin@<hostname>
   admin@<hostname>'s password:
   ```

   where *hostname* is the hostname (for example. KB-C0-01-01) or IP address of the device.
2. Enter **control** mode:

   ```
   KB-C0-01-01> control
   KB-C0-01-01(control)>
   ```
3. Query the TFTP server to determine if firmware on the server is newer than firmware on the device:
   ```
   KB-C0-01-01(control)> software check server_ip <IPv4-address-of-TFTP-server>
   KB-C0-01-01(control)>
   ```
4. If newer firmware is available, a message will be displayed:
5. `update available: 2.8.0, image file: <firmware_filename>`

   The firmware filename consists of three parts:

   <product_name>-<device_family_name>-<version_number>

   where:

   - *product_name* is **kb_sw-prod**
   - *device_family_name* is one of:
     - **NOMAD** — Firmware used for D621 and P621 devices.
     - **DEVO** — Firmware used for C410, C420, and P421 devices.
   - *version_number* is the version number of the firmware.

   For example:

   kb_sw-prod-DEVO-2.8.0
6. Upgrade the software:
   ```
   software upgrade server_ip <IPv4-address-of-TFTP-server>
   ```

After the software upgrade completes, the device will reboot.

Upgrade from the REST API

1. Download and unzip the upgrade files from Altowav Altoplex Firmware Downloads at support.altowav.com.

   The following files are included in the zip file:

   - A digest file
   - The firmware file

   The firmware filename consists of three parts:

   <product_name>-<device_family_name>-<version_number>

   where:

   - *product_name* is **kb_sw-prod**
   - *device_family_name* is one of:
     - **NOMAD** — Firmware used for D621 and P621 devices.
     - **DEVO** — Firmware used for C410, C420, and P421 devices.
   - *version_number* is the version number of the firmware.

   For example:

   kb_sw-prod-DEVO-2.8.0

2. Upload the firmware image file to a server that can be access by all devices.
3. Use the `configuration/software_upgrade` API to install the firmware file. For example:
   `curl -k -X POST -u admin:<password> -H "Content-Type:application/octet-stream" -H "X-File-Name:<path>/<filename>" --data-binary @<path>/<filename> https://<hostname>/rest/v002/configuration/software_upgrade`

   Where:

   - *password* is the password to log into the device. The default password is **admin**.
   - *path* is the path to the firmware file. If the command is executed from the same local directory as the firmware file, path is not necessary.
   - *filename* is the name of the firmware upgrade file, for example, kb_sw-prod-DEVO-2.8.0.
   - *hostname* is the hostname or IP address of the device being upgraded.

   The following example curl command uses the `-i` option to show the response headers, and demonstrates that the file transfer was successful and that the upgrade has begun:

```
$ curl -i -k -X POST -u admin:admin \
-H "Content-Type:application/octet-stream" \
-H "X-File-Name:kb_sw-prod-DEVO-2.8.0.plain" \
--data-binary @kb_sw-prod-DEVO-2.8.0.plain \
https://10.0.0.01/rest/v002/configuration/software_upgrade
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 34.1M 100 88 100 34.1M 15 6358k 0:00:05 0:00:05 --:--:-- 6301kHTTP/1.1
100 Continue
HTTP/1.1 200 OK
Content-Type: application/json
```

```
Cache-Control: public, must-revalidate, proxy-revalidate
Content-Length: 88
Date: Sat, 01 Jan 2022 00:23:39 GMT
Server: lighttpd/1.4.73
{
"status":"starting",
"running-sw-version":"2.7.0",
"upgrade-running":"yes"
}
```

The upgrade may take up to several minutes to complete.

Verify that the firmware update was successful

Verify firmware update from the command line

1. log in via ssh to the P421:

   ```
   $ ssh admin@<hostname>
   admin@<hostname>'s password:
   ```

   where *hostname* is the hostname (for example. KB-C0-01-01) or IP address of the device.

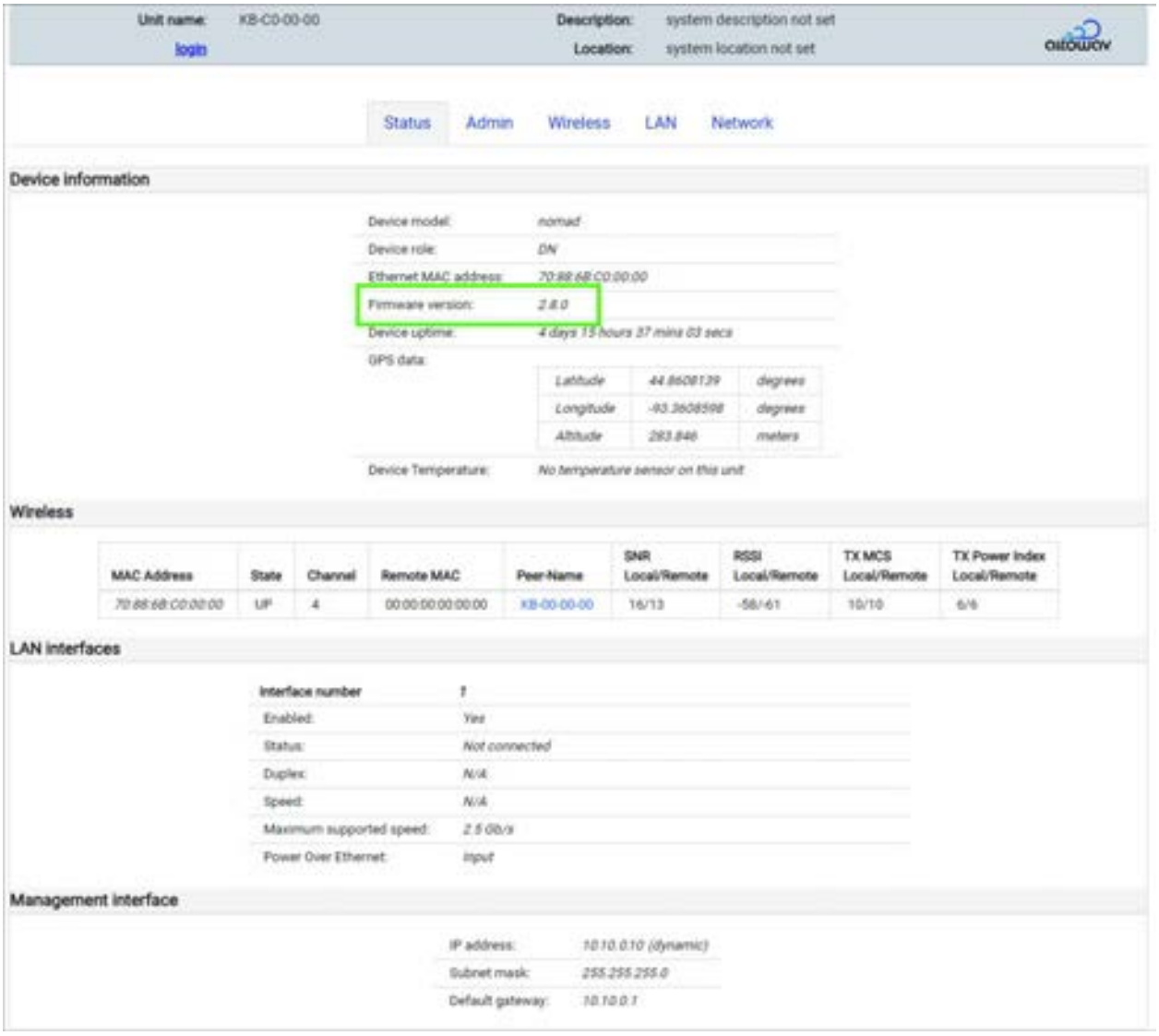
2. Check the status of the device by using the **kb_device_status** command:

   ```
   KB-C0-01-01> kb_device_status
   [Device: KB-C0-01-01, HW name: devo, software: 2.8.0]
   description: test iteration 32
   location: system location not set
   authorized_org:
   led_enable: enable
   date: Wed Oct 9 14:32:24 UTC 2024
   uptime: 14:32:24 up 3 days, 16:07, 1 users, load average: 1.10, 1.11, 1.09
   DNS Servers: 10.80.0.252
   Radio Link:
   Radio Local MAC          Local Intf  Remote MAC         Status CN
   ----- ------------------ ----------- ------------------ ------ -----------
   wlan0 00:00:00:00:00:00  terra0      00:00:00:00:00:01  UP     KB-C0-00-02
   KB-C0-01-01>
   ```

   Verify that the software version matches the expected value of the upgrade.

Verify firmware update from the WebUI

1. Open the WebUI.
2. The firmware version is displayed on the **Status** page in the **Device Information** section:



Verify firmware update form the REST API

Use the device/node_identity API to return the firmware version:

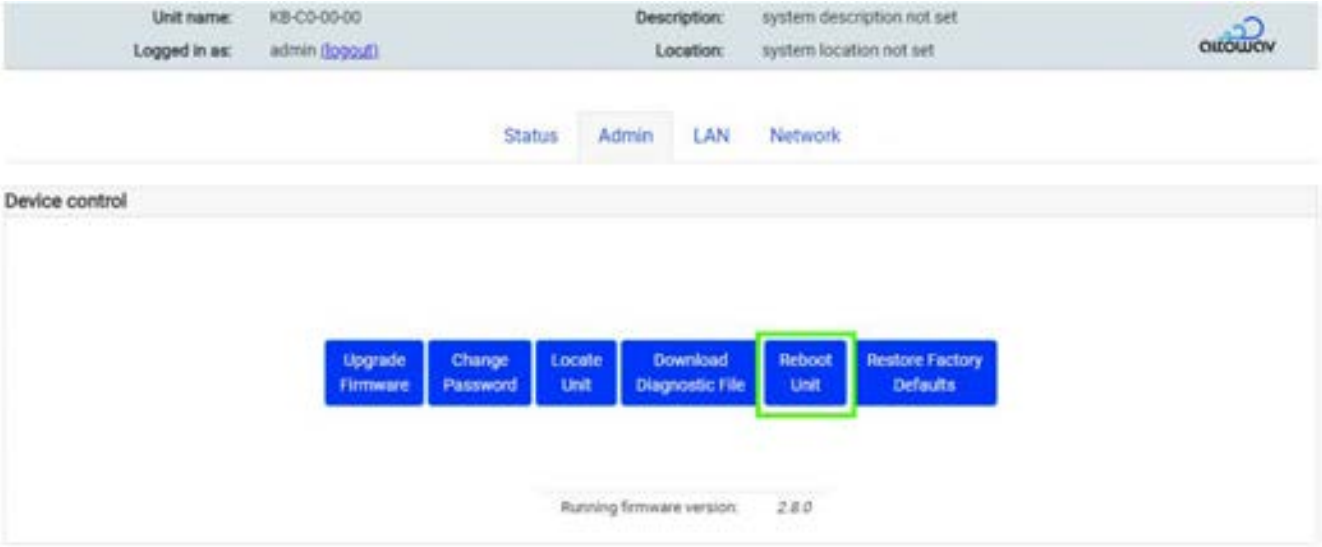
```
$ curl -k -u admin:admin https://KB-C0-01-01kb-c0-00-e6/rest/v002/device/
node_identity
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   605  100   605    0     0   8188      0 --:--:-- --:--:-- --:--:--  8402{
  "Ethernet MAC" : "70:88:6B:C0:00:00",
  "HW name" : "devo",
  "HW rev" : 2,
  "HW type code" : 82,
  "Node role" : "DN",
  "Number Ethernet Interfaces" : 1,
  "Number RF Interfaces" : 1,
  "Part number" : "1900-8411-1012-devo-2-LBKA0ZZ1SV1",
  "Serial number" : "00000000000000000001KB-C0-00-00:2",
  "authorized_org" : "",
  "bootloader version" :
"KBBLVERSION:1.3:prod:robot:2024-10-09_11-57-10:devo:1b565eb",
  "description" : "system description not set",
  "gps available" : 1,
  "location" : "system location not set",
  "name" : "KB-C0-01-01",
  "node type" : "PTP",
  "software" : "2.8.0"
}
```

Reboot

Note: A power-cycle or reboot clears the diagnostic log information stored in the device. So during troubleshooting, you should capture the diagnostic log in a file, before the power-cycle or reboot. If you require troubleshooting assistance, information in the diagnostic log may be useful.

1. P421 devices default to DHCP for IP assignment. Access the WebUI by browsing to the hostname or IP address. For example, type **https://<hostname>/** in the browser's address bar.
2. Click the **login** link in the WebUI header to log in as administrator. The username is **admin**, and the default password is **admin**.

3. Click on the **Admin** tab, entering the password to log in when prompted.
4. Click on the **Reboot Unit** button in the **Device control** section and wait until the reboot is complete.



> **Tip:** View the **Wireless** table on the **Status** tab to verify that links for this device have come up again.

If you are unable to reach the device's WebUI but are near the unit and can physically disconnect it from power, a power cycle will perform a hard reboot of the device.

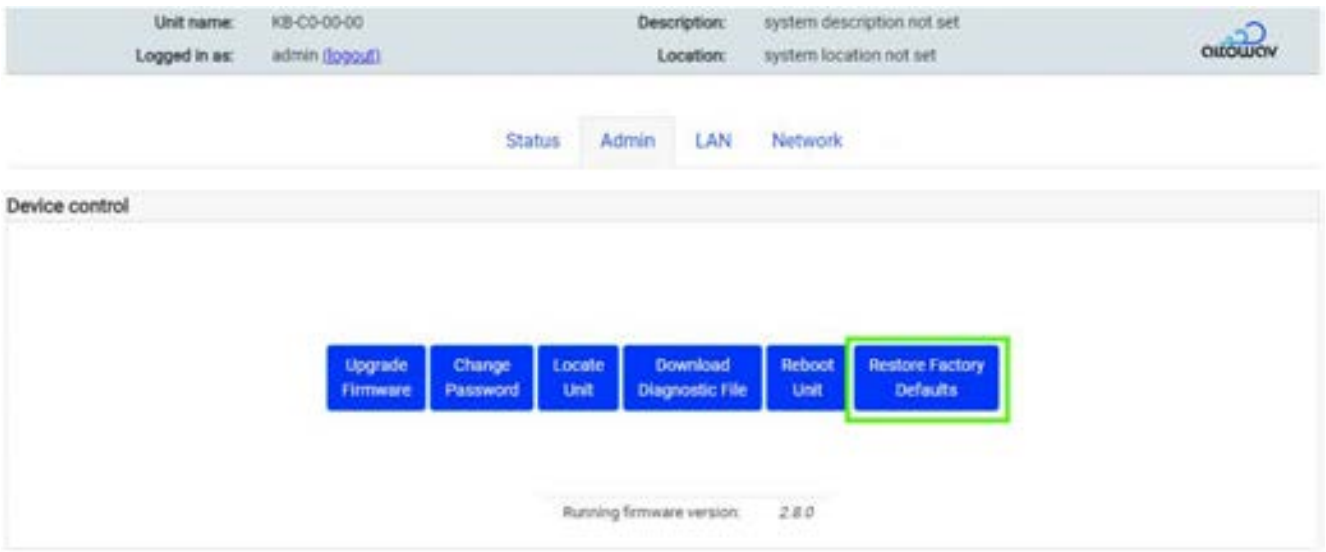
Factory Reset

Restore factory defaults by using the WebUI

Use the **Restore Factory Defaults** button in the device's WebUI to perform factory reset.

1. P421 devices default to DHCP for IP assignment. Access the WebUI by browsing to the hostname or IP address. For example, type **https://<hostname>/** in the browser's address bar.
2. Click the **login** link in the WebUI header to log in as administrator. The username is **admin**, and the default password is **admin**.

3. Click on the **Admin** tab, entering the password to log in when prompted.
4. Click on the **Restore Factory Defaults** button in the **Device control** section and wait until the reboot is complete.



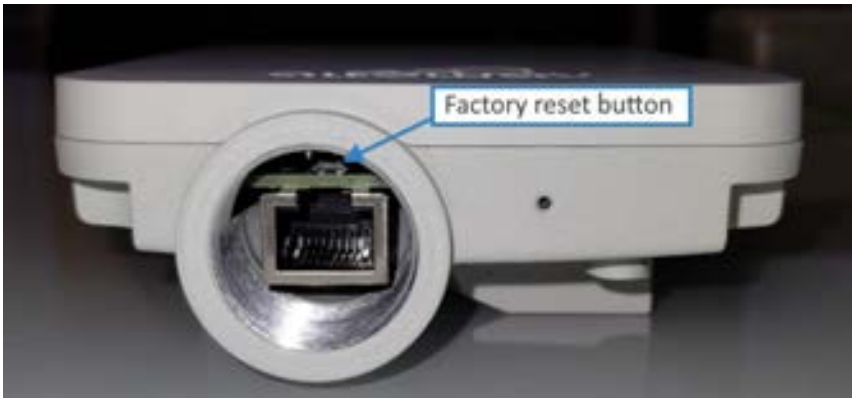
Restore factory defaults by using the factory reset button

If the WebUI is inaccessible due to a lost password or in cases where network settings are inadvertently set to unworkable values, use the following hard factory reset steps:

After the reset, normal operation resumes with factory default settings.

Hard factory reset requires the following:

- Access to the reset button via an uncovered port on the device.
- The device must be connected to power over Ethernet (PoE). (The following image is disconnected from PoE to show the reset button location.)
- Ability to hold the reset button and cycle the power at the same time.



Follow these steps to perform a hard factory reset.

1. With the device powered up, insert a pin into the Factory reset button inside Port 1 above the RJ45. Push down and hold.
2. Cycle the power to the device while holding the reset button.

3. Continue to hold the reset button down, until the LEDs flash a red and green sequence. Then remove the pin from the reset button. This may take up to 40 seconds.
4. The LED is solid red while the device boots. This may take up to 2 minutes.
5. When the LED flashes green the reset is complete.

After the reset, normal operation resumes with factory default settings. The login credentials for the device return to **admin**.

Troubleshooting

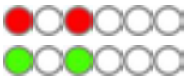
This chapter contains the following topics:

LED Indicators

The P421 is equipped with a single LED, showing both red and green lights to indicate power, connection and activity.

The light sequences indicate the state of the unit. The following table shows the meaning of the light sequences.

LED behavior		Indicates
	Solid red	Device is powering up.
	Slow flashing green	Device is waiting for GPS to synchronize. If the device is the wireless responder, the LED will stop slow flashing once a connection to the wireless initiator has been established, whether or not GPS has synchronized on the responder.
	Flashing green	Device is waiting to form a wired connection and at least one wireless connection.
	Solid green	Device has a wired connection and at least one wireless connection.
	Flashing red/green	Device is in locate mode.
	Flashing red/green, pausing, then flashing red/green again.	Device is booting and ready for the factory reset button to be pressed. The device will stay in this mode for approximately ten seconds, or until the factory reset button is pressed. See Factory Reset for information about performing a factory reset.

	Flashing red, pausing, then flashing green, pausing, then repeating.	The factory reset button has been pressed and the device is performing a factory reset.
	Flashing red, pausing, then repeating.	Error condition.

Lost Password

If a P421 device password is lost, the device may have to be reset to factory defaults.

After the reset, operation resumes with factory default settings, including the default password: **admin**.

Download a Diagnostic File

Altowav is committed to providing high quality technical support. If you encounter an unusual issue that you cannot easily solve through standard troubleshooting, please contact us at support@altowav.com with the following information:

- Your contact information.
- The type and model of hardware with the issue.
- Product serial number.
- A description of the issue.

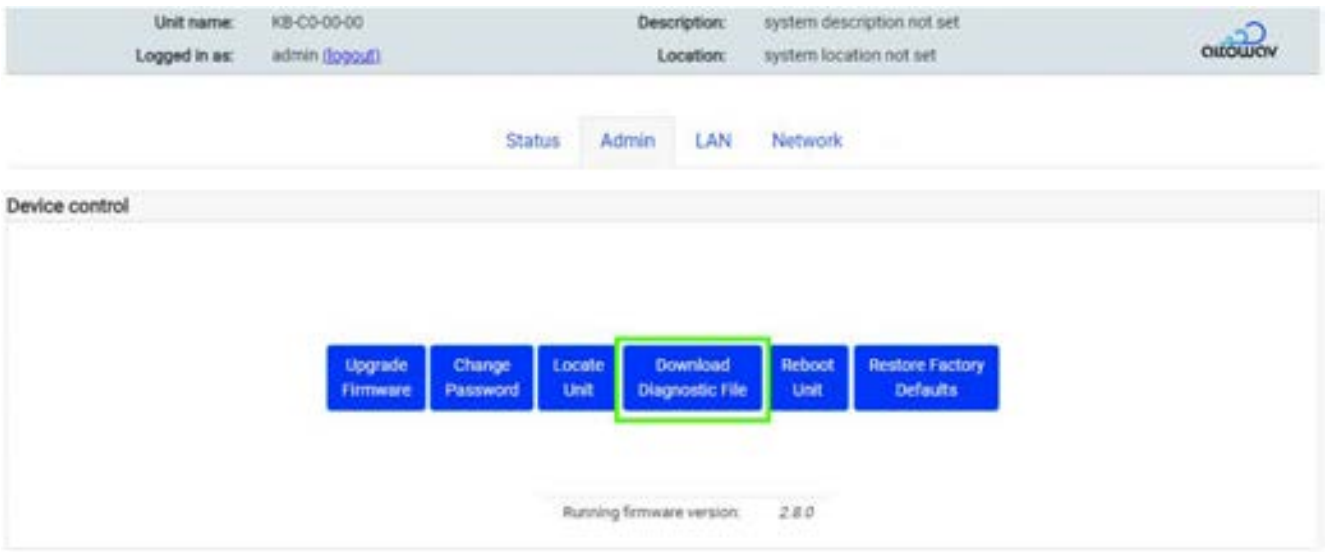
We also recommend that you provide a diagnostic log of device interactions and conditions.

Note: A diagnostic log file captures historical information about a device's operation. It is important to download the diagnostic file before rebooting or power-cycling a device as part of troubleshooting. Rebooting or power-cycling will clear the log file history.

Follow these steps to download a diagnostic file for connected devices from the WebUI:

1. P421 devices default to DHCP for IP assignment. Access the WebUI by browsing to the hostname or IP address. For example, type **https://<hostname>/** in the browser's address bar.
2. Click the **login** link in the WebUI header to log in as administrator. The username is **admin**, and the default password is **admin**.

3. Click on the **Admin** tab, entering the password to log in when prompted.
4. Click on the **Download Diagnostic File** button in the **Device control** section and wait until the reboot is complete.



1. The file is sent to your system's default download location. The file name includes the host name (KB MAC) of the device and the date. For example, KB-C0-01-01_diag_2024-10-09-20-32-26.txt
2. Zip the file and attach it to an email to support@altowav.com or a ticket at support.altowav.com.

Create a diagnostic file from the REST API

1. Use the `admin/diagdump` API to create a diagnostic file from the REST API. For example, use the curl command to save the diagnostic information to a file named `diag_dump`, created in the current directory:
   `curl -k -o diag_file.txt -u admin:<password> https://<hostname>/rest/v002/admin/diagdump`

   where:

   - *password* is the password to log into the device. The default password is **admin**.
   - *hostname* is the hostname or IP address of the device.
2. Zip the file and attach it to an email to support@altowav.com or the ticket at support.altowav.com.

Wi-Fi Connection

Connect to a P421 via diagnostic Wi-Fi to access the WebUI for configuration tasks, if required.

Some uncommon scenarios where this may be useful:

- If the device's WebUI is unreachable via standard access methods. This could happen if Network settings were inadvertently set to unworkable values, or if a direct connection is not feasible due to where the unit is mounted.
- When a device must be reset to factory defaults with the Hard Reset method, a Wi-Fi connection may be useful to reconfigure settings after the reset.

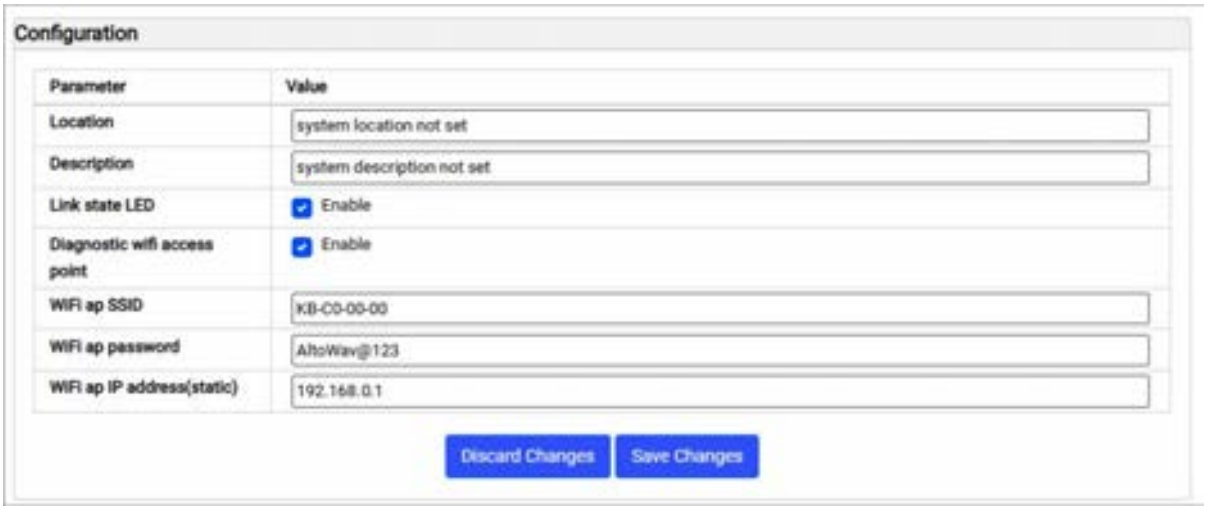
- After the initial install of a device, if links do not come up as expected per your design, a Wi-Fi connection could be used to verify and update configurations. This may be especially helpful in cases where the unit is rotated, resulting in sector orientation that is different from the design plan, or in cases where bench configuration was done improperly.

  > **Tip:** To avoid this issue, make sure links come up as part of the installation process.

- In rare cases, the distribution node could become unreachable after configuration and operation in a network. If the unit cannot be reached via wireless or Ethernet link, the unit may be reachable via Wi-Fi.

Wi-Fi Settings

Settings for diagnostic Wi-Fi access are in the Configuration section of the Wireless tab of the WebUI.



Default for diagnostic Wi-Fi access point is enabled.

Default Wi-Fi ap SSID is the Host Name of the device. (Listed as HN: KB-XX-XX-XX on the device label.)

Default Wi-Fi ap password is **AltoWav@123**

Default Wi-Fi ap IP address is 192.168.5.1 (static IP for the device's Wi-Fi access point).

Prerequisites for connecting to the D621 via Wi-Fi:

- You must be in close range to the P421 in order to connect to it via Wi-Fi — generally within 10 - 20 ft.
- A P421 allows only one incoming connection to Wi-Fi at a time. If multiple technicians are on site, only one may be connected.

To access a device via Wi-Fi:

1. Scan for possible Wi-Fi connections.
2. Find the device's hostname and select **Connect**.
3. Enter the **Wi-Fi ap password**.
4. Browse to the device's **Wi-Fi ap IP address** to open the WebUI.

The WebUI opens to the **Status** tab. Standard device login is required to view any other tab of the WebUI or access settings.