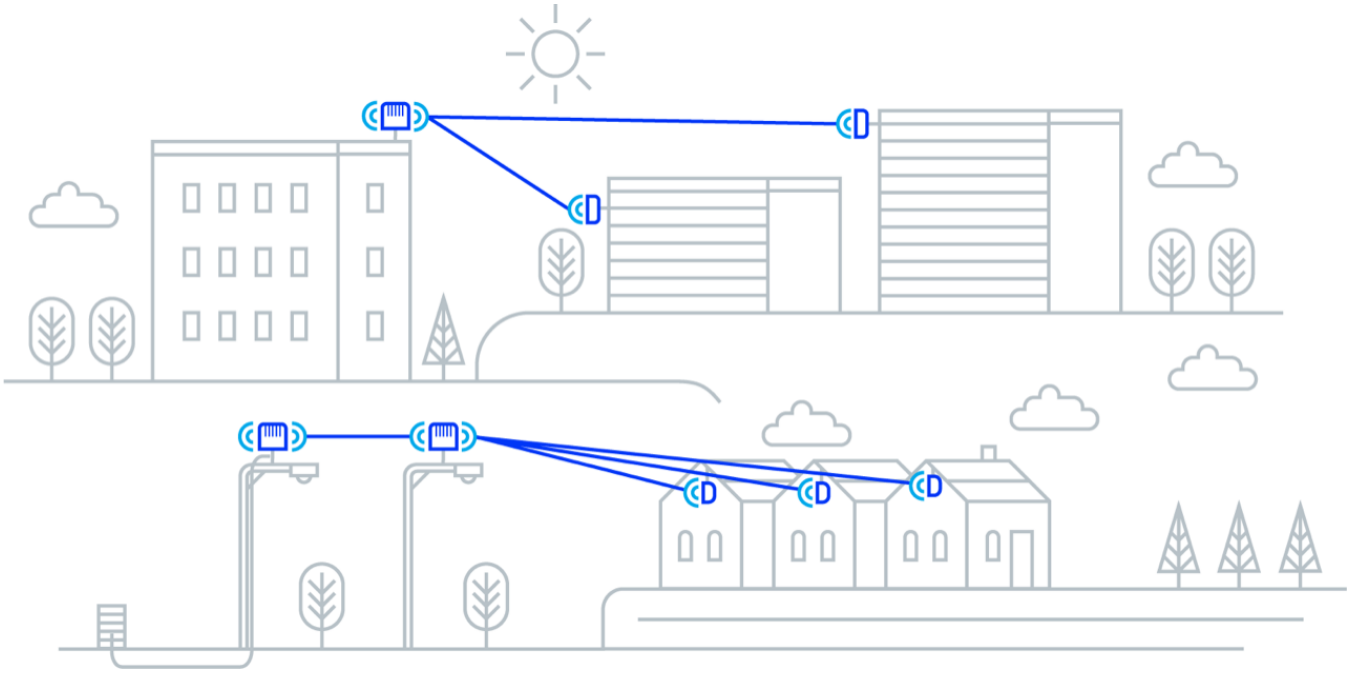


Altowav

C423 User Guide

Version 4.2.0

April 4, 2026

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 C423.

Altowav™, AltoPlex™, and AltoCommand™ are trademarks of Altowav Inc. Kwikbit™, and Kwikbit Networks™ are trademarks of Kwikbit Internet.

All trademarks, logos and brand names are the property of their respective owners.

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 C423.

Regulatory statements

FCC Radiation Exposure Statement

The C423 device complies with FCC radiation exposure limits set forth for an uncontrolled environment. A minimum of 35 centimeters (14 inches) of separation between the C423 and all persons shall be maintained.

FCC Regulatory Statement

The C423 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 C423 device complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. A minimum of 35 centimeters of separation between the C423 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 C423 et toutes les personnes doit être maintenu.

ISED Industry Canada Regulatory Statement

The C423 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 or satellites (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 ou de satellites (l’Annexe J de la norme ISED RSS-210).

EU regulatory notes

This product meets the technical requirements of EC Decision (2006/771/EC) on harmonization of the radio spectrum for use by short range devices, band number 75a with operation between 57 GHz and 66 GHz and a maximum radiated transmit power of 40 dBm e.i.r.p.

Altowav has issued Declarations of Conformity for this product. See support.altowav.com for further information.

Specific guidelines with regard to outdoor operation of 60 GHz radios vary by EU member country. Refer to the radio regulatory agency in the country of operation for more information.

This product includes a 2.4 GHz radio with operation between 2412-2472MHz frequency range and a maximum radiated transmit power of 19.99 dBm e.i.r.p.

⚠ Changes or modifications to this equipment not approved by Altowav or the party responsible for compliance could void the user's authority to use the product.

⚠ Outdoor radios should be installed by experienced installation professionals who are familiar with local building and safety codes, and who are, when applicable, licensed by the appropriate regulatory authorities. Failure to do so may void the product warranty and may expose the end user or the service provider to legal and financial liabilities. Altowav and its resellers and distributors are not liable for injury, damage, or violation of regulations associated with the installation of outdoor radios.

Recommended radio frequency exposure exclusion zone

In compliance with the ICNIRP 2020 Guidelines and the following regulations for limiting exposure to electromagnetic fields:

- USA — FCC 47CFR1.1310
- Canada — ISED Safety Code 6 (2015)
- Europe — EC Recommendation (1999/519/EC) and Directive 2013/35/EU
- The following table lists the recommended RF exposure exclusion zone for the C423:

General public/Uncontrolled environment	Occupational/Controlled environment
35 cm	15cm

Restrictions statement

BE	BG	CZ	DK	DE	EE	IE
EL	ES	FR	HR	IT	CY	LV
LT	LU	HU	MT	NL	AT	PL
PT	RO	SI	SK	FI	SE	UK(NI)
NO	IS	LI	CH	TR		

For the European Union, you must check with your national authority for any restrictions. Restrictions may apply in some countries where outdoor use is not allowed. Licensing is required for the UK prior to use.

Revision history

Revision	Date
• Initial release of the C423	4/04/2026

Contents

C423 User Guide overview

Thank you for choosing the Altowav AltoPlex series for your fixed-point networking solution. This user guide describes installation, configuration and operation of the C423 device.

This guide is intended for network and system administrators who will install, configure, and manage Altowav networks using C423 devices.

This guide includes instructions for the installation, configuration and management of the C423 device 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 C423 and other AltoPlex devices:

- For general technology specifications and product datasheets, see altowav.com/technology/
- C423 Quick Start Guide
- D621 User Guide
- Altowav AltoCommand User 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.

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).
- Surveillance camera connectivity.
- Multi-dwelling unit distribution.

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

C423 installation and configuration

The installation instructions for C423 radio includes:

- Tool list.
- C423 box contents.
- Mounting instructions.
- Functional description.
- A list of the network design information required.
- Installation and configuration steps.
- Configuration example.

Tool List

- 8mm nut driver or slotted screwdriver for band clamp.
- #2 Phillips head screwdriver for wall mount.

Box contents

- C423 device.
- IP67 cable glands.
- QR code card for C423 Quick Start and User Guide.

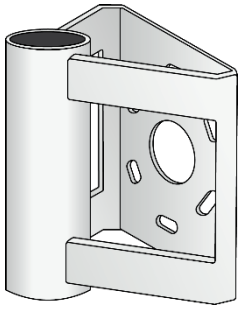
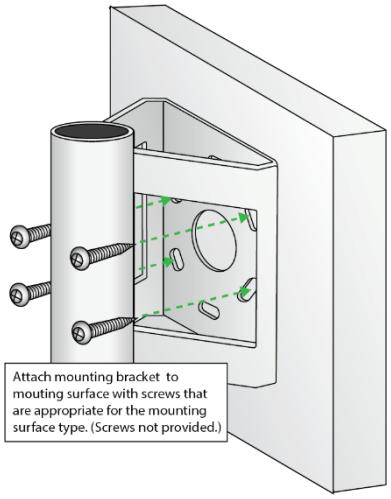
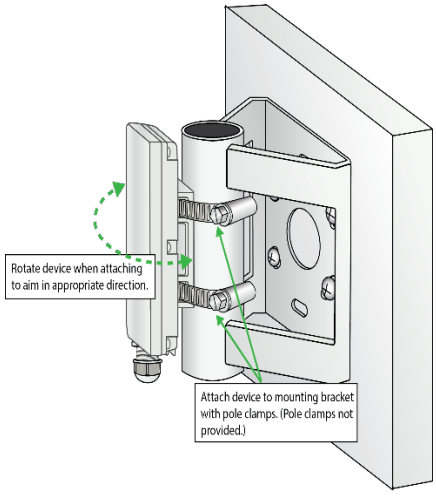
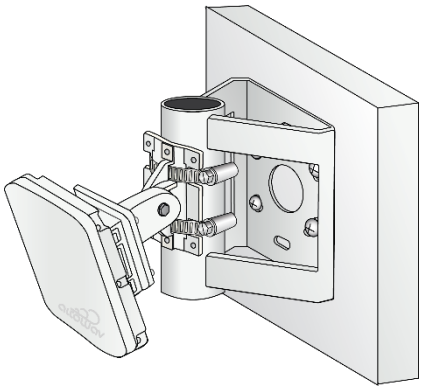
Mounting brackets

Altowav offers two optional mounting brackets. The two mounting brackets can be used together to provide both azimuth and elevation control.

- The Altowav Wall Mount, model number AX-AW3-MT-WALL.
- The AltoPlex Extended Range Pole Mount, model number AX-AW3-MT-EXT.

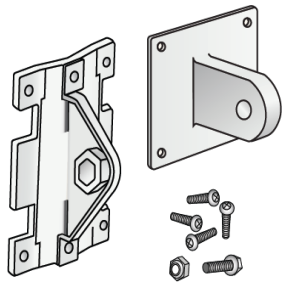
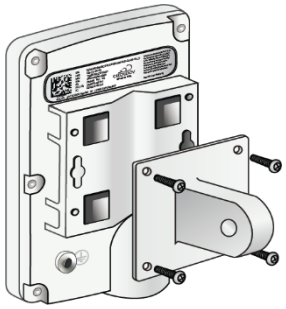
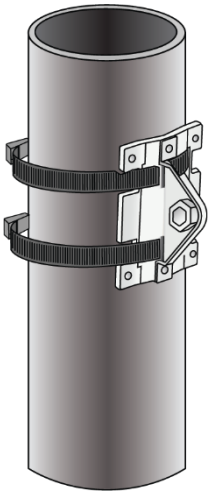
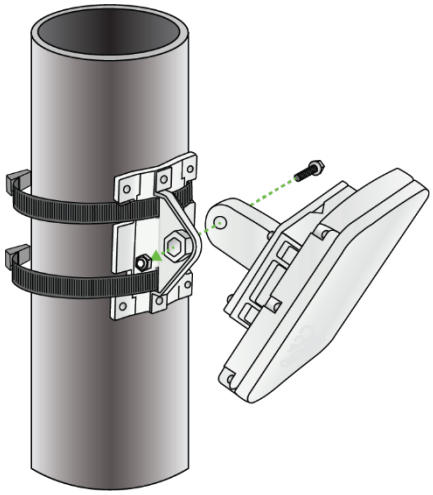
Altowav Wall Mount

The Altowav Wall Mount, model number AX-AW3-MT-WALL, can be used to securely mount the C423 to a wall or similar flat surface. It can also be used in tandem with the AltoPlex Extended Range Pole Mount to provide both azimuth and elevation control.

Bracket	Attach to wall or flat surface
	
Attach the C423 to wall mount	**Optional installation with the AltoPlex Extended Range Pole Mount**
	

AltoPlex Extended Range Pole Mount

The AltoPlex Extended Range Pole Mount, model number AX-AW3-MT-EXT, enables secure installation and elevation adjustments from +60° to -45°. This model can be used for pole mounting with screws, bolts, or band clamps, and can also be used in tandem with the Altowav Wall Mount, as show above.

Bracket	Attach to the C423
	
Pole mounting with band clamps	
	

About the C423

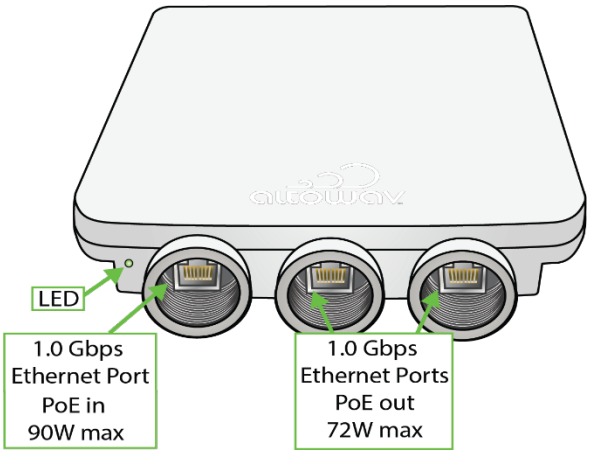
The C423 is a client node (CN) that work in tandem with the D621 distribution node (DN) to provide 60GHz wireless networking connectivity, giving fiber speeds at a fraction of the cost and with rapid deployment. Both models have the same durable and weatherproof outer case.

The 1.0 Gbps RJ45 ports and LED are located at the base of the unit.

The red/green LED on the bottom of the C423 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.



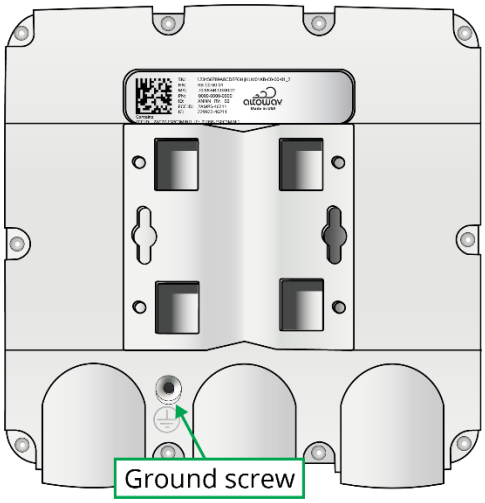
Requirements for deployment

These items are required to form a wireless link with an AltoPlex device that is running in distribution node (DN) role:

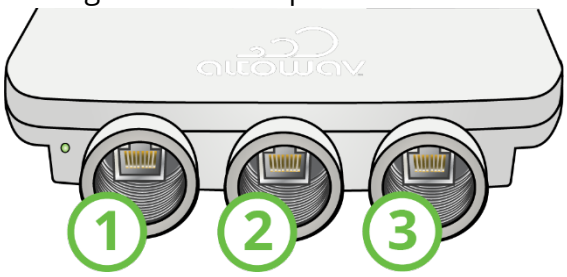
- Clear line of sight (LOS) to the distribution node.
- The hostname of this device (KB-XX-XX-XX). Listed as **HN:** on the device label.
- WebUI, CLI, or REST API access to the distribution node for configuration of the client node.

Installation steps

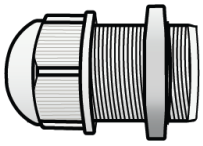
The C423 device is designed to work out of the box and should not need bench configuration prior to installation and connection.

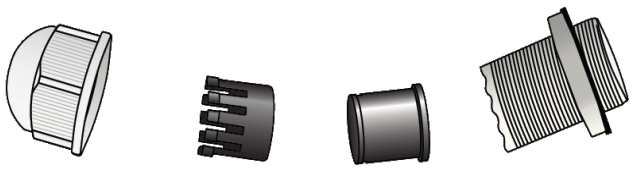


1. Install the ground wire, if required by code, at the installation location. Connect the other end of the ground wire to nearby good earth. The ground screw on AltoPlex devices is a #6-32 5/16th inch Phillips head screw.
2. Install an outdoor-rated Ethernet cable through the provided cable gland and into port 1 on the C423 device:

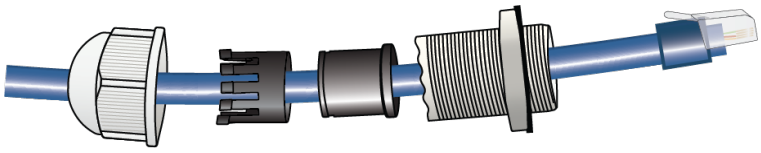


A. Unscrew and deconstruct the components of the gland.

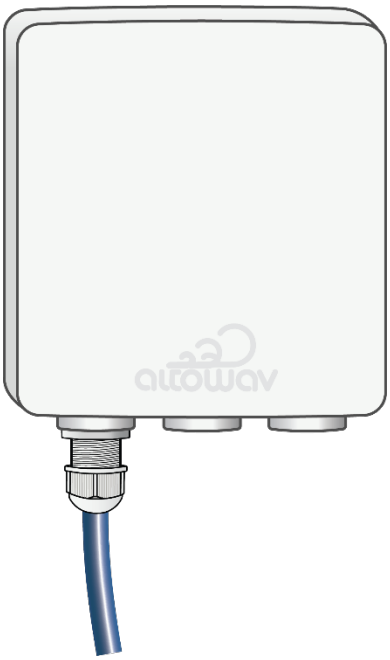


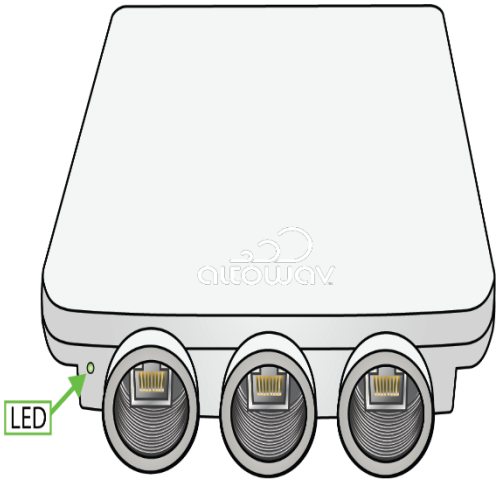


B. Insert an outdoor-rated Cat5e (minimum) cable in the gland as shown.



   C. Secure the components of the gland and attach the Cat5e cable to the device's RJ45 port and attach the gland to the device. Do not overtighten.
2. Repeat the above steps as necessary for ports 2 and 3.
3. Mount the device to a wall or pole at the installation location with the mounting bracket (see Mounting bracket). Ensure a clear line of sight to the connecting distribution node and no obstructions to GPS above the unit. Orient the C423 according to the planned azimuth and elevation.
4. Connect the Ethernet cable from port 1 to a CE certified, standard IEEE Type 4 802.3bt Class 8 90W Power over Ethernet (PoE) injector or PoE switch.
5. Verify that the device powers up. (LED is red during boot-up and then flashing green.)

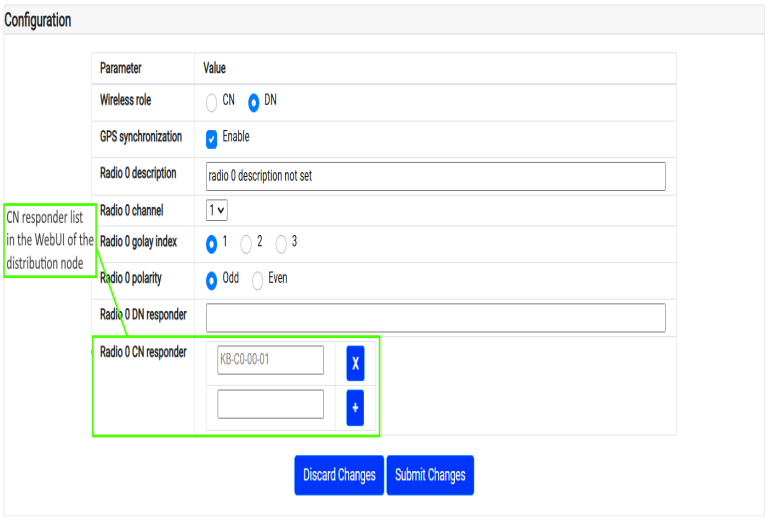




Add the C423 as a client node to a distribution node

The C423 can only operate as a client node (CN) that is attached to a distribution node (DN). This connection is configured on the distribution node after the client node has been installed. This section describes how to add the C423 to a distribution node and complete and verify the installation.

1. Add the hostname (KB-XX-XX-XX) of the device to the **CN Responder** list of the connecting distribution node to initiate a link. In the distribution node's WebUI, the **CN Responder** list is on the **Wireless** tab. Click **Submit Changes**.



   The wireless link is formed with no further configuration on the C423 device, provided that:

   - The line of sight to the distribution node is clear.
   - Network settings for Management VLAN are the same for both devices. The factory defaults work for this.

2. After the device connects, review and configure its settings. With the wireless link active, this can be done remotely. C423 Configuration via WebUI provides options for how to access the C423 WebUI.
   A. Set the Location and Description on the Admin tab.
   B. Review settings on the **LAN** and **Network** tabs and adjust as required.
3. Verify the operation of the new device and review its performance. Adjust for line of sight, and rebeamform as needed. Dress the cable and power cord securely to avoid wear.

Connecting to the C423

By default, AltoPlex radios use dynamic IP address assignment and, beginning with release 3.6.0, have a factory default fallback static IP address of 192.168.0.1.

Additionally:

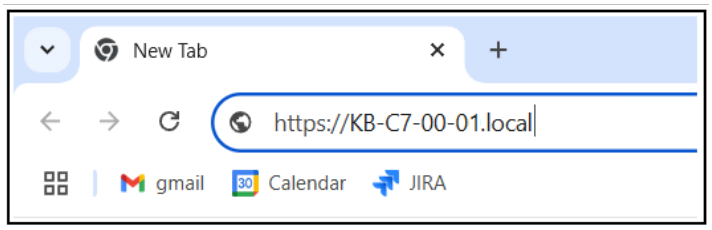
- Radios can be configured to use a static IP address, rather than dynamic IP address assignment. This will override the fallback IP unless the radio is factory reset. After a factory reset, it will return to default behavior.
- Radios upgraded to release 3.6.0 that have not been factory reset will have a factory default fallback IP address of 192.168.0.51, unless they have a configured static IP address that overrides the default address. After a factory reset, they will have the default behavior.
- Radios at a release earlier than 3.6.0 have a unique factory default IP address that is printed on the label affixed to the front of the radio at manufacturing time.

Note: You can determine if your radio was manufactured before release 3.6.0 based on the IP address printed on the label on the front of the radio:

- If the radio was manufactured before the release of 3.6.0, the IP address on the label will be a unique IP address.
- If the radio was manufactured after the release of 3.6.0, it will either not have an IP address on the label, or the IP address will be 192.168.0.1.

Because AltoPlex radios participate in multicast DNS (mDNS), computers that support mDNS and are on the same subnet as the radio can connect to the radio by using its hostname. In general, this should work regardless of whether the radio is configured to use dynamic or static addressing, or if it is using the fallback default IP.

For example, if your radio's hostname is KB-C7-00-01 and your computer is on the same subnet as the radio, you can access the WebUI by typing **https://KB-C7-00-01** (or **https://KB-C7-00-01.local**) into your browser's URL address bar:



Use the factory default fall-back IP address to connect to the radio

This section applies to radios with firmware version 3.6.0 or newer. Radios with older firmware have a unique fallback link local IP address that was provided on a printed label when the device was manufactured. For devices originally manufactured with a software version prior to 3.6.0 and then upgraded to release 3.6.0 or newer, the default IP address will depend on whether the device has been factory reset since the upgrade:

- If the device has not been factory reset, the default IP address is 192.168.0.51.
- If the device has been factory reset, the default IP address is 192.168.0.1.

To connect to an AltoPlex radio by using its default fallback IP address:

1. Configure your computer to be a member of the 192.168.0.*x* subnet.

   For example, on Windows 11:

   A. Click the **Windows** icon.
   B. Click Settings.
   C. Click Network & internet.
   D. Click Ethernet.
   E. For IP assignment, click Edit.
   F. Select **Manual**.
   G. Click to toggle on **IPv4**.
   H. For **IP address**, type an address in the 192.168.0.*x* subnet (for example, **192.168.0.2**).
   I. For Subnet mask, type 255.255.255.0.
   J. Click **Save**.

2. Next, either:
   - Plug your computer's Ethernet connection into the **LAN** port of a PoE injector that is connected to the radio.

     Tip: The LAN port is sometimes labeled as the **Data out** port, the **Out** port, or something similar.

   - Plug both your computer and the radio into a PoE switch.

     Tip: To access the radio by using the default IP address, make sure that the switch is not connected to the backhaul network or that the backhaul network does not have a DHCP server running on it.

3. Access the radio's WebUI by entering either the hostname (for example, **https://KB-C7-00-01**) or the default IP address (**https://192.168.0.1**) in the address bar of a web browser.

   Note: If a radio has a configured static IP address that is different than the default address, the configured IP address must be used to access the radio.

4. A warning message may indicate that the self-signed certificate used by the device is not recognized by the browser. Instructions to clear the message vary depending on the browser. For example, in Chrome:

A. Click Advanced.
B. Click Proceed to...

The WebUI will open with the **Status** tab displayed.

Determine the IP address of a radio by using mDNS

If you configure a radio to use a static IP address and subsequently do not remember the IP address, you can use mDNS commands to determine the radio's IP address.

Note: This requires that your computer supports mDNS and is on the same subnet as the radio.

- Windows Powershell:

  Resolve-DnsName <hostname>

- MacOS:

  dns-sd -G v4v6 <hostname>

- Linux:

  avahi-resolve-host-name -4 <hostname>.local

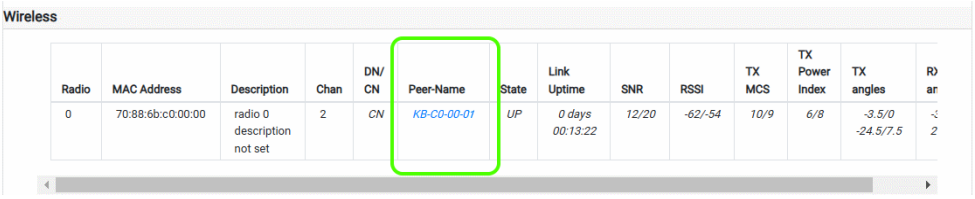
  where <hostname> is the hostname of the AltoPlex radio (KB-XX-XX-XX).

C423 Configuration via WebUI

During installation, the hostname (KB-XX-XX-XX) of the C423 device is added to the **CN responder** list for the specific distribution node (DN) device to which it connects. That configuration change for the distribution node initiates the wireless link between the the distribution node and the C423 client node.

After the C423 link to the network is active, you can access the WebUI using one of the following methods:

- Link from the WebUI of the connected distribution node (DN). On the **Status** page of the connected distribution node, in the **Wireless** section, click on the device listed in the **Peer-Name** column.



- Access the WebUI of the C423. In your browser's address bar, type:

  https://*hostname*

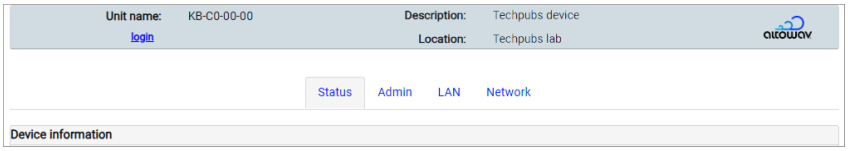
  where *hostname* is the hostname (KB-XX-XX-XX) or IP address of the radio. See Connecting to the for more information.

- If using the AltoCommand web-based management tool, access the WebUI from the **Devices** page. On the row of the device to configure, click the menu icon in the settings column and click **Connect to Device**.

General startup configuration steps for the C423 often include:

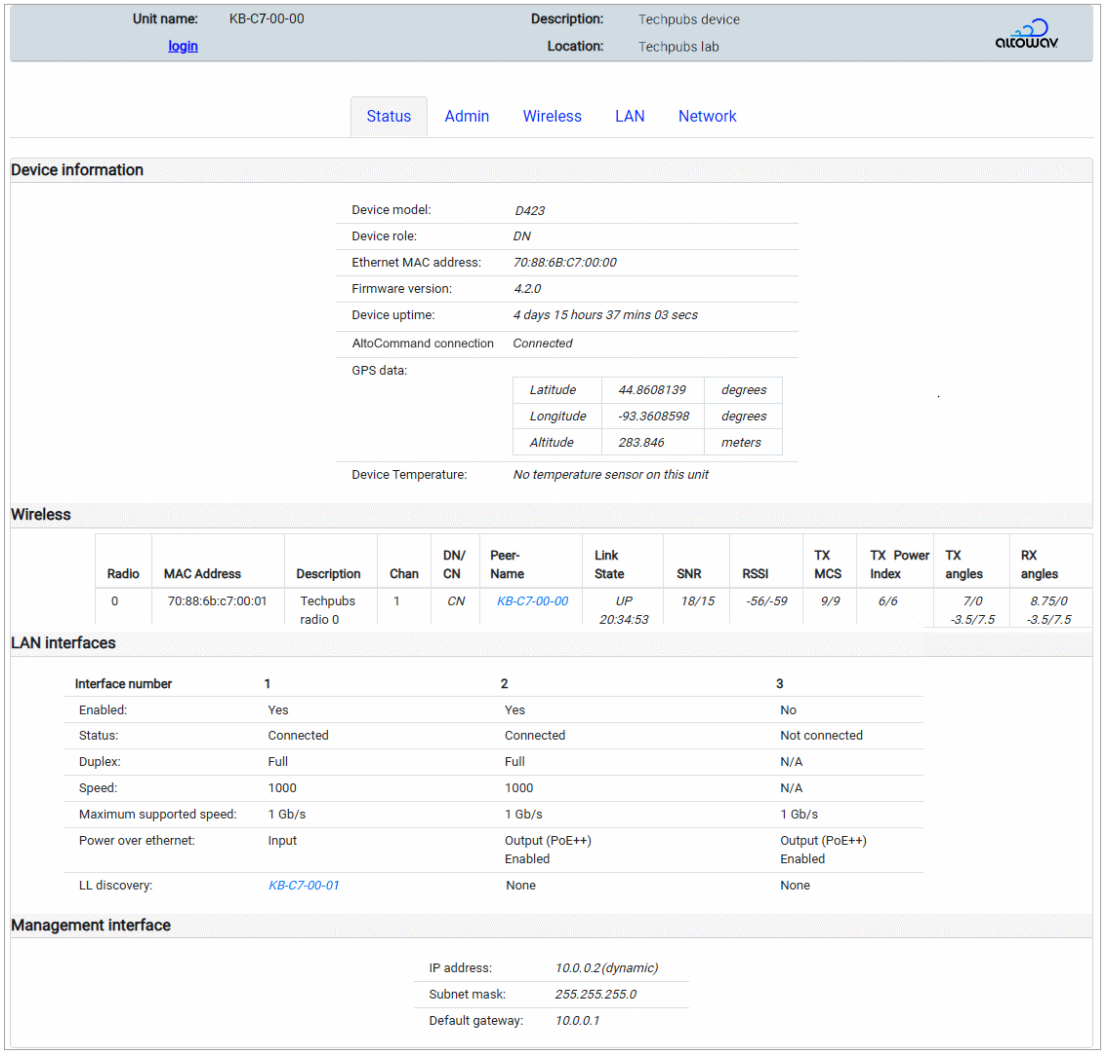
- Click on the **Admin** tab and do one or more of the following:
  - Upgrade Firmware
  - Change Password
  - Set the **Location**
  - Set the Description
- On **Network** tab, set network configuration items for the management network interface and VLAN.

The header of the WebUI shows the **Unit Name** of the device, (also called the hostname), **Description** and **Location**, as well as offering a login link. Login is not required to view read-only information about the device, but is required to set configurations on any other tab of the WebUI.



Status tab

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



Status tab — Device information

This section describes the model of the device, the device's role (CN — client node), Ethernet MAC address, firmware version, device uptime, status of its connection to the AltoCommand server, GPS information, and device temperature.

Note: The AltoCommand server is configured on the distribution node.

Status tab — Wireless

Displays information about the device's wireless connection to a distribution node.

Status tab — LAN interfaces section

This section shows information for the LAN interfaces (3 ports for the C423), including whether the port is enabled, its status (**Connected** or **Not connected**), duplex mode, speed, maximum supported speed, and PoE mode.

If the device's Ethernet port is connected via a switch to other AltoPlex devices, the hostnames of connected devices will be included in the **LL Discovery** field. Clicking a device's hostname in the **LL Discovery** field will open the WebUI for that device. This is useful to determine which devices are co-located (for example, devices that are installed on the same pole).

Note: **LL Discovery** requires that the devices are connected by an unmanaged switch, or a managed switch that is configured to forward LLDP packet information.

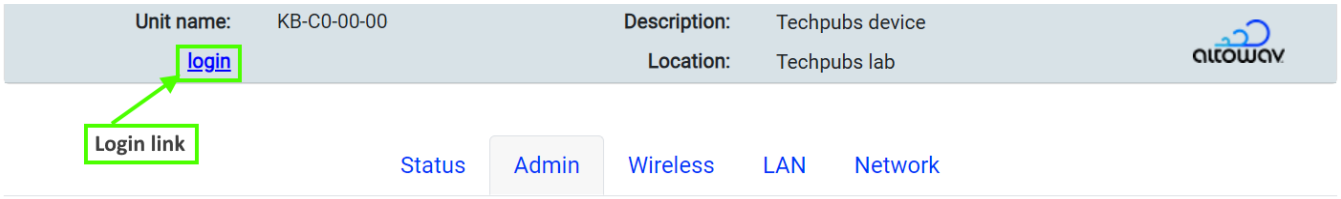
Status tab — Management interface

This section lists the IP address and whether the address is dynamic or static, the subnet mask, and default gateway for the management interface on the node.

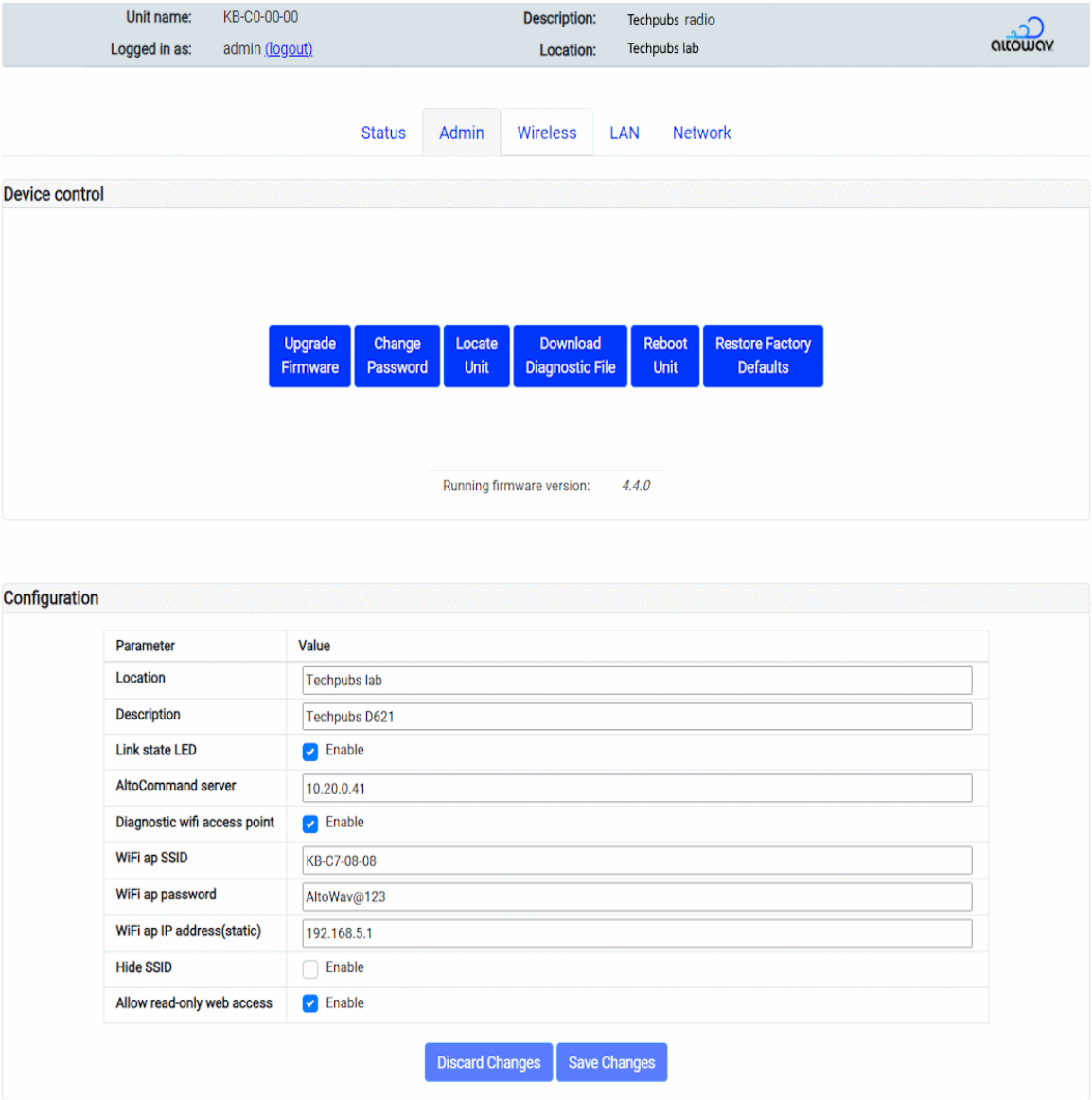
Admin tab

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 default password is **admin**.

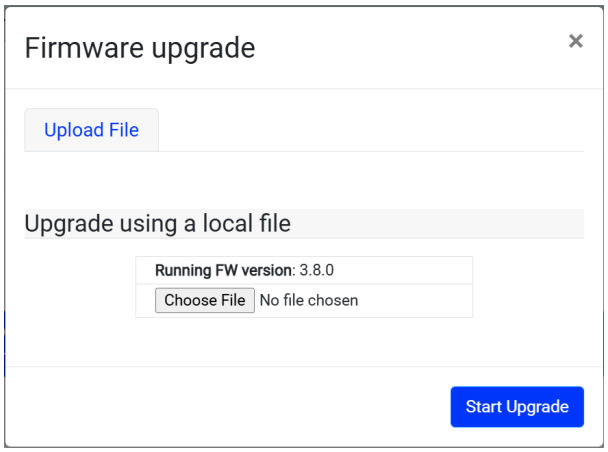


The **Admin** tab has two sections: **Device control** and **Configuration**.



Admin tab — Device control section

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



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

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. See the AltoCommand User Guide for more information.

Change Password — Use this button to change the password for the admin of the C423. See Change a device password for instructions.

Locate Unit — Click this button to put the unit into locate mode. In locate mode, the device flashes the LED in a specific sequence so that field personnel can identify the unit. The LED sequence is: LED flashes 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-C7-00-01_diag_2025-12-04-14-43-32.txt, means this is the diagnostic text file for the device KB-C7-00-01, created at 2:43:32 pm (UTC) on December 4, 2025. See Download a Diagnostic File for instructions.

Reboot Unit — Restarts the unit remotely. See Reboot for instructions.

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, unless it has been configured to use a static IP address.

Admin tab — Configuration section

This section includes the following settings:

Location — Use this field to describe the physical location where the device is installed. Allows up to 130 characters.

Description — Use this field to provide a description of the device. This 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. Allows up to 130 characters.

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 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). Allows up to 32 characters.

WiFi ap password — Sets the password for the diagnostic Wi-Fi access. Default setting: AltoWav@123. Allows between 8 and 63 characters.

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

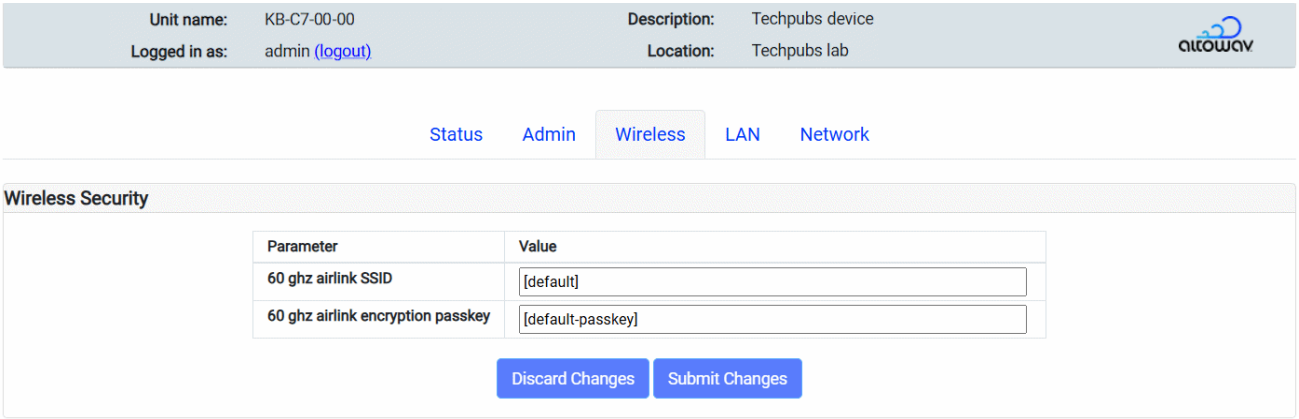
Wireless tab

You can change the 60 GHz airlink SSID and encryption passkey from the **Wireless** tab.

All AltoPlex devices have the same default SSID and encryption passkey for their 60 GHz airlink. Generally, this is sufficient because the devices will only form links to radios that are specified in their configuration.

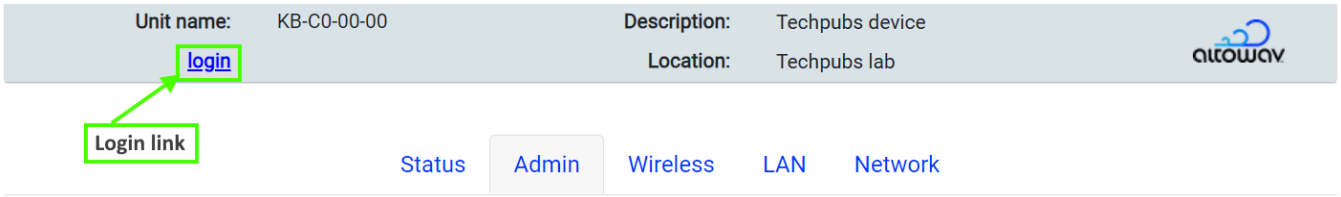
All linked radios must have the same SSID and encryption passkey. If you change the SSID and/or passkey, they must be changed for all linked radios or the links will not form.

Note: When changing the SSID and passkey for radios that are already installed in the field, begin with client nodes, and then the most remote distribution nodes, moving backwards towards the point of presence. This insures that you will have access to all radios during the process.



To change the SSID and encryption passkey for the 60 GHz airlink:

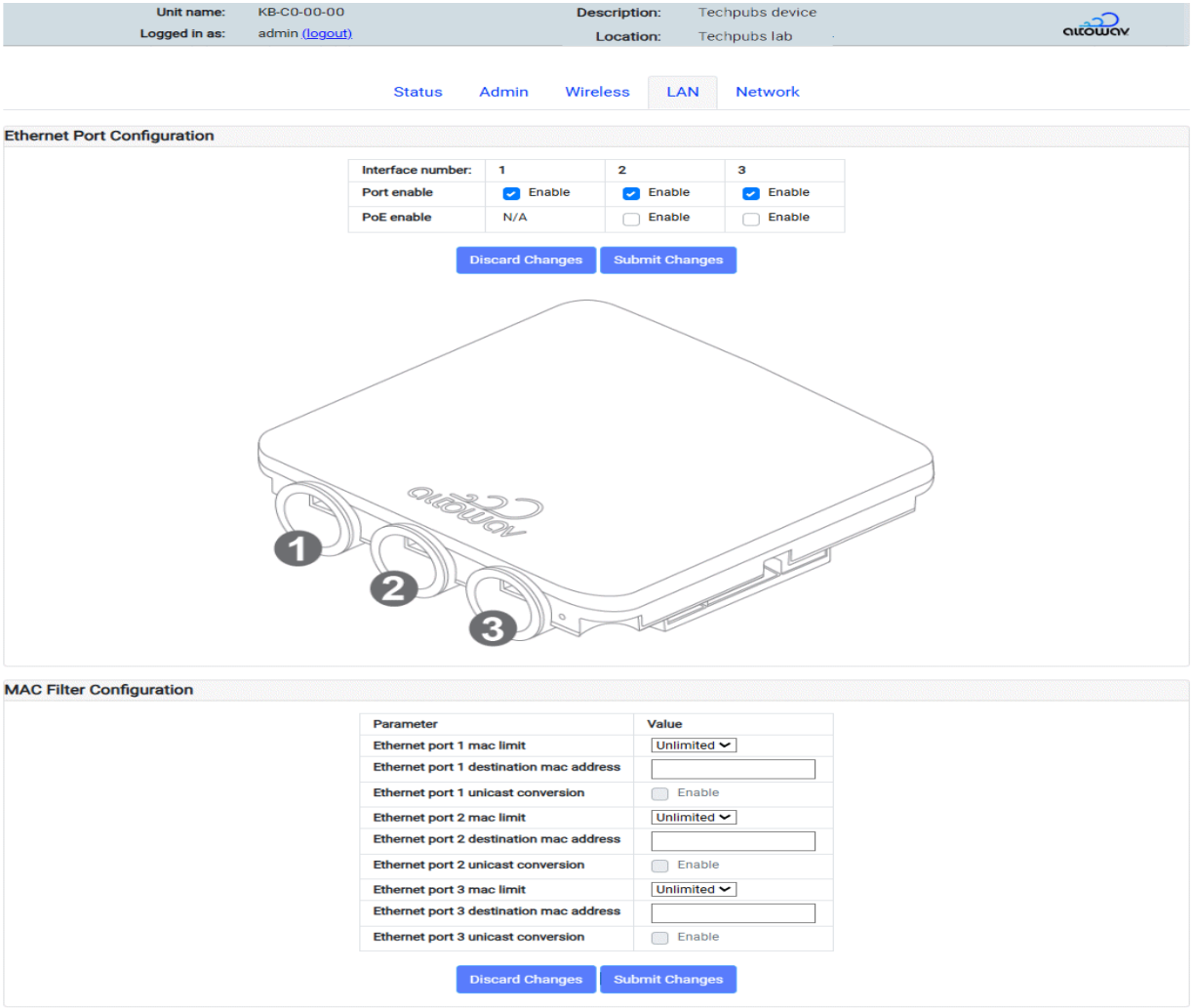
1. Click the **login** link in the WebUI header to log in as administrator. The default password is **admin**.



2. For **60 GHz airlink SSID**, type the new SSID.
3. For **60 GHz airlink encryption passkey**, type the new encryption passkey.
4. A confirmation screen will remind you that the SSID and passkey must be the same for all linked devices, and will indicate that the device will reboot in order to complete the change. Click **Yes** to confirm.

LAN tab

The LAN tab provides settings for enabling Ethernet traffic on the LAN port for the C423.



LAN tab — Ethernet Port Configuration

Port enable — Determines whether the specified port is enabled for data transmission.

PoE enable — For port 2 and 3, determines whether the port is enabled for PoE output.

- Notes:
  - The maximum output of each port is 70.4W. If the output exceeds 70.4W, the port will lose power.
  - The combined maximum output of both ports is 78 watts.
    - Assumes 90 watts of PoE input on port 1, and 12 watts required to power the device.
    - If the maximum power output of ports 2 and 3 combined exceeds the maximum available power, this will cause the device to fail to operate.
  - The actual amount of available power will vary based on environmental factors, such as the wattage provided by the PoE injector, and the length of the Ethernet cable connecting the PoE injector to port 1.
  - In the WebUI, hover over the port in the graphic to show the current connection status of the port.

LAN tab — MAC Filter Configuration

AltoPlex radios support both source and destination MAC filtering.

- **Source MAC filtering** — Configures the radio to forward network traffic on a specific Ethernet port only if the traffic is originating from specific MAC addresses.

  On AltoPlex radios, source MAC filtering is configured by setting the number of allowed MAC addresses (up to 10 are supported). The radio then automatically populates an allowlist that contains the first devices that connect to the Ethernet port, up to the configured limit. Traffic is not forwarded from any devices not on the allowlist.
  - You clear the allowlist by either rebooting the radio or making a change to the configuration, at which point a new allowlist will be automatically created.
- **Destination MAC filtering** — Configures the radio's individual Ethernet ports to only forward unicast network traffic to a specified destination MAC address. Network traffic with a destination MAC address that matches the configured MAC will be forwarded. All other network traffic will be dropped.

  You can also configure the radio to convert broadcast and multicast traffic into unicast and forward it to the configured destination MAC address. This may be useful for certain types of broadcast or multicast network traffic, such as DHCP requests.

Configure MAC filtering

In the **MAC Filter Configuration** section of the **LAN** tab, for each Ethernet port:

1. Configure source MAC filtering:
    A. For **Ethernet port *x* mac limit**, select the number of MAC addresses to be included in the allowlist. Allowed values are **1**-**10** and **Unlimited**. The default is **Unlimited**, which means that source MAC filtering is disabled.
    B. An allowlist is automatically generated based on the first MAC addresses that connect to the device after source MAC filtering is enabled, up to the configured limit.
        - You can repopulate the allowlist by rebooting the radio or making a configuration change.
        - See Show the current MAC filter configuration for information about how to determine the current source filter allowlist.
2. Configure destination MAC filtering:
    A. For **Ethernet port 1 *x*destination mac address**, type the destination MAC address that unicast network traffic must contain for the traffic to be forwarded.
    B. For **Ethernet port 1 *x*unicast conversion**, click **Enable** to convert broadcast and multicast network traffic to unicast and forward that traffic to the specified destination MAC address.
3. Click Submit Changes.

Show the current MAC filter configuration

You can show the current MAC filter configuration, including the current allowlist that the radio is using for source MAC filtering, by using either the CLI or the REST API.

- CLI:
    1. Log in via ssh to the D423:

        $ ssh admin@<*hostname*>

        admin@<*hostname*>'s password:

        where *hostname* is the hostname (for example, KB-C7-00-01) or IP address of the radio. See **Error! Reference source not found.** for more information.

    2. Use the **mac_filter_status** command:

```
KB-C7-00-01> mac_filter_status
  kb_name: KB-C7-00-01
  ports:
    eth1:
      filter_eth1_destination_mac: 70:88:6B:C7:00:02
      filter_eth1_unicast_conversion: enable
      filter_eth1_source_mac_limit: 4
      source_mac_allowlist:
        a0:b1:c2:d3:e4:f5
```

```
      0a:1b:2c:3d:4e:5f
      ff:ee:dd:cc:bb:aa
      00:11:22:33:44:55
    eth2:
     filter_eth2_destination_mac: 70:88:6B:C7:00:02
     filter_eth2_unicast_conversion: enable
     filter_eth2_source_mac_limit: 4
      source_mac_allowlist:
       a1:b2:c4:d5:e5:f6
       1a:2b:3c:4d:5e:6f
       aa:bb:cc:dd:ee:ff
       55:44:33:22:11:00
    eth3:
     filter_eth3_destination_mac:
     filter_eth3_unicast_conversion: disable
     filter_eth3_source_mac_limit: unlimited
     source_mac_allowlist:
KB-C7-00-01>
```

- REST API:

  Use the **device/mac_filter_status** API. For example:

  1. In your browser, type the following URL in the address bar:

     https://<*hostname*>/rest/v002/device/mac_filter_status?output=text

     where *hostname* is the hostname (for example, KB-C7-00-01) or IP address of the radio.

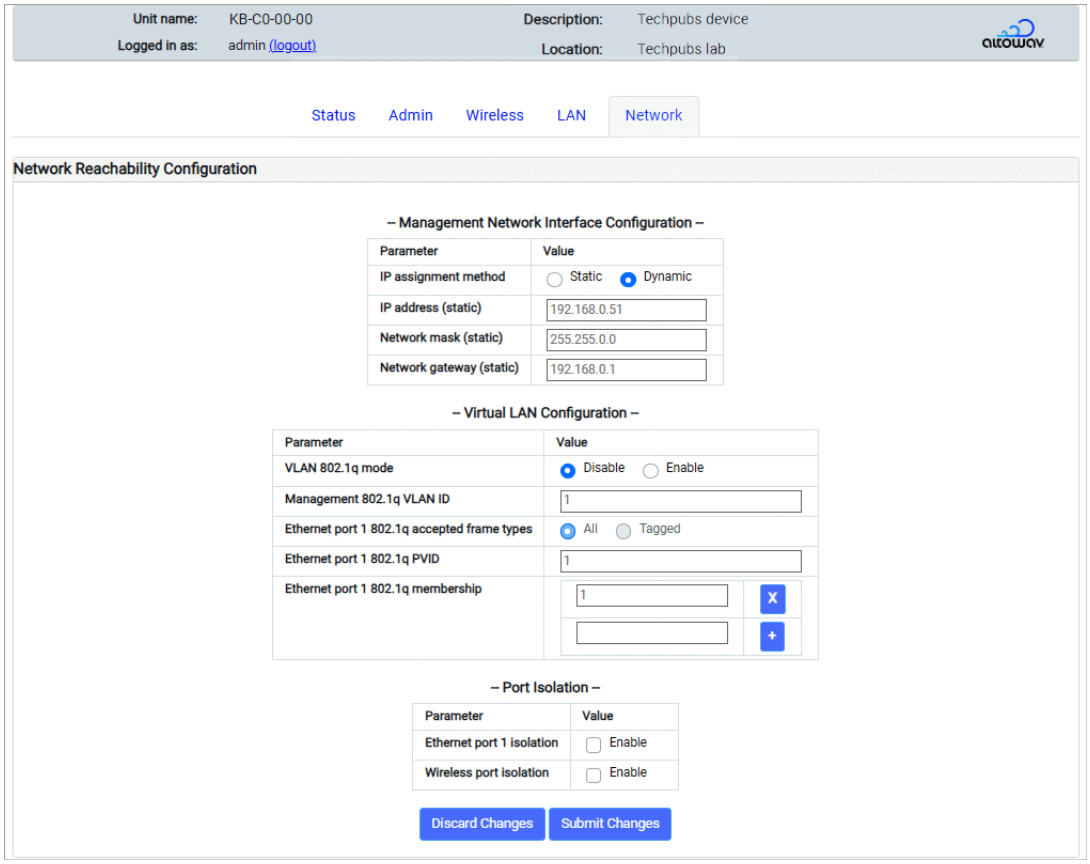
  2. The following output is displayed in the browser window:

```
kb_name: KB-C7-00-01
 ports:
  eth1:
   filter_eth1_destination_mac: 70:88:6B:C7:00:02
   filter_eth1_unicast_conversion: enable
   filter_eth1_source_mac_limit: 4
   source_mac_allowlist:
    a0:b1:c2:d3:e4:f5
    0a:1b:2c:3d:4e:5f
    ff:ee:dd:cc:bb:aa
    00:11:22:33:44:55
  eth2:
   filter_eth2_destination_mac: 70:88:6B:C7:00:02
   filter_eth2_unicast_conversion: enable
   filter_eth2_source_mac_limit: 4
   source_mac_allowlist:
```

```
    a1:b2:c4:d5:e5:f6
    1a:2b:3c:4d:5e:6f
    aa:bb:cc:dd:ee:ff
    55:44:33:22:11:00
  eth3:
   filter_eth3_destination_mac:
   filter_eth3_unicast_conversion: disable
   filter_eth3_source_mac_limit: unlimited
   source_mac_allowlist:
```

Network tab

The **Network** tab offers settings for Management Network Interfaces, VLAN configuration and Port Isolation, as well as additional Layer 2, SNMP, Network Services, and DHCP settings. The **Network** tab has a long list of settings, so the images below show only one section at a time with brief descriptions following.



Note: Adding a C423 device's hostname (KB-XX-XX-XX) to the **CN responder** list in a distribution node's (DN) configuration initiates the wireless link between the DN and the C423. These devices are designed to work with other AltoPlex devices out of the box.

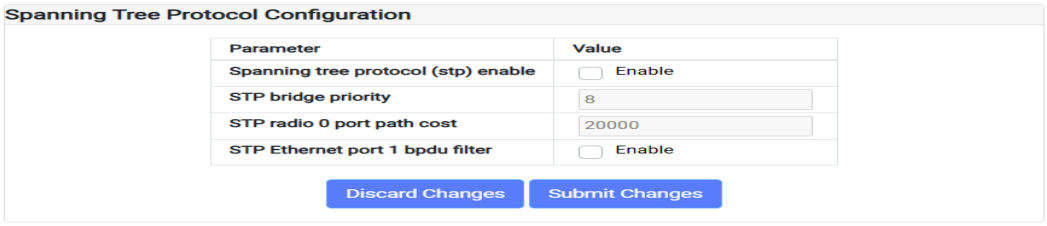
Network tab — Network Reachability Configuration

Management Network Interface Configuration — IP assignment method is Dynamic by default. If set to **Static**, the IP address, network mask and network gateway must be set.

Virtual LAN Configuration — Enable/disable the 802.1q VLAN mode, setting VLAN IDs, accepted frame types, PVIDs and memberships as required for your specific network operation.

Port Isolation — Enable/disable the port isolation for each port interface on the unit by checking/clearing the box.

Network tab — Spanning Tree Protocol Configuration



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.

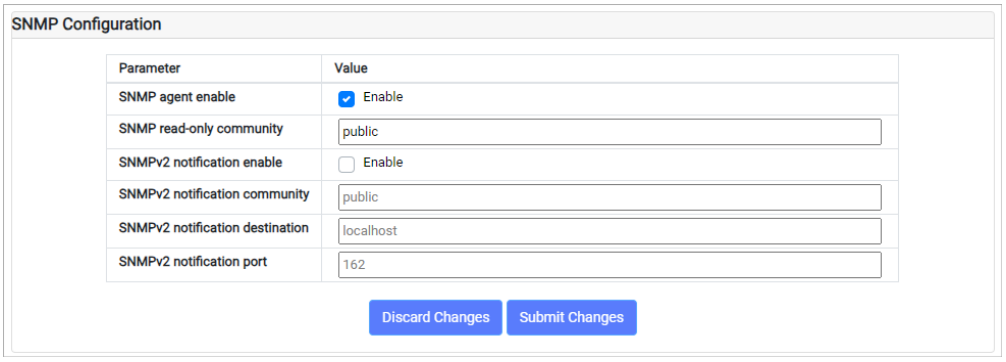
STP bridge priority is used to determine which device will serve as the root of the spanning tree. The device with the lowest priority will serve as the root. The priority configured here is a multiplier; to determine the actual STP priority, multiply by 4096.

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

The **STP Ethernet port 1 bpdu filter** prevents BPDU packets from being forwarded, which allows for separate networks to be isolated from participating in the same STP environment. When enabled, the filter is applied whether or not Spanning Tree Protocol is enabled.

Network tab — SNMP Configuration

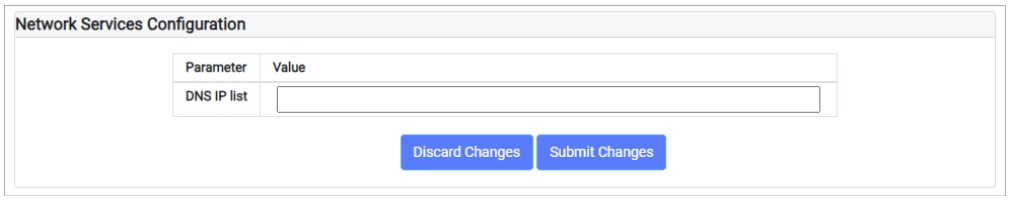
Simple Network Management Protocol (SNMP) is used to monitor devices on a network for performance and error information. The settings in this section enable/disable SNMP and configure notification and community access settings.



The Altowav enterprise MIB can be downloaded at https://www.altowav.com/technology/assets/pdf/ALTOWAV-MIB.mib.

Network tab — Network Services Configuration

DNS IP list — A list of DNS server IP addresses using commas to separate the addresses.



Network tab — DHCP Relay Configuration (Option 82)

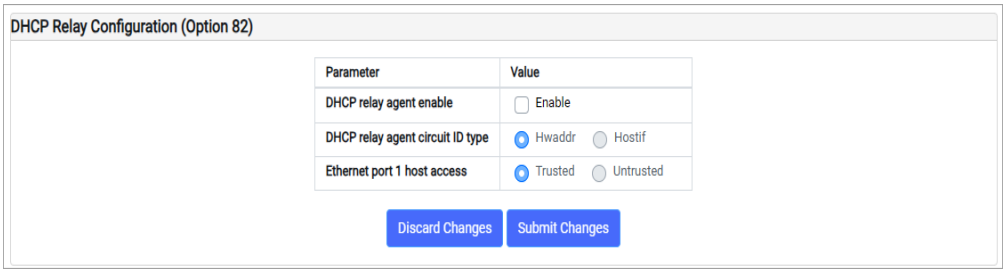
Enable the DHCP relay agent to:

- Prevent unauthorized DHCP servers from serving IP addresses to devices on your network.
- Insert a circuit ID into a DHCP message that identifies the source of the message. The **DHCP relay agent circuit ID type** can be either **HWaddr** (the MAC address of the / C423's Ethernet port, in ASCII format), or the **Hostif** (the hostname:Ethernet_port of the C423 in ASCII format).

You can also select whether the Ethernet port is:

- **Trusted** — All DHCP packets coming from devices attached to the Ethernet port will be forwarded.
- Untrusted:
  - All DHCP server packets from attached devices will be blocked.
  - All DHCP client packets from attached devices that have option 82 information in their header will be blocked.
  - All DHCP client packets from attached devices that do not have option 82 information in their header will be fowarded, with the circuit ID appended.

Note: All wireless links are automatically considered trusted.



Maintenance and security

Wi-Fi connection to a C423

Connect to a C423 via Wi-Fi to access the WebUI for diagnostic purposes and configuration tasks, if required.

Note: The Wi-Fi connection to the C423 provides a connection to the device for management and diagnostic purposes. It does not provide a connection to the an external network, or to the internet.

Some scenarios where this may be useful:

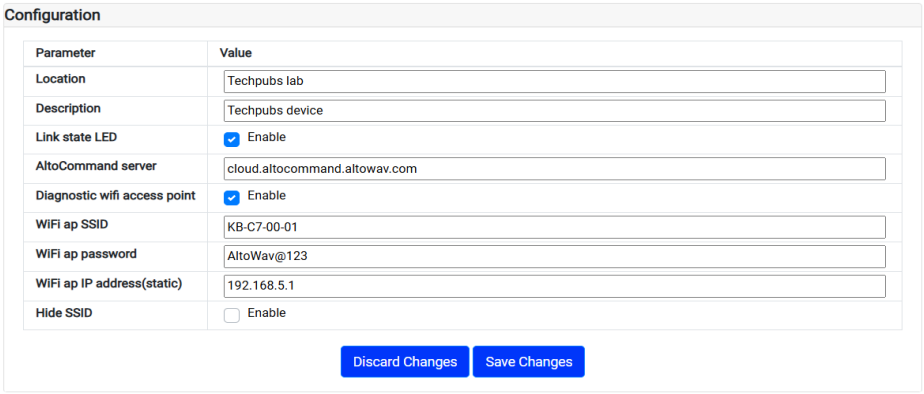
- If the device's WebUI is unreachable via standard access methods. This could happen if Network settings were inadvertently set to unworkable values, or if a direct connection is not feasible due to where the unit is mounted.
- When a device is reset to factory defaults, a Wi-Fi connection may be useful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

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 Wi-Fi access are in the Configuration section of the **Admin** tab of the WebUI.



Default for Diagnostic Wi-Fi access point is enabled.

Default **Wi-Fi ap SSID** is the hostname 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. This is the static IP for the device's Wi-Fi access point.

If **Hide SSID** is enabled, the Wi-Fi SSID will not be broadcast.

Prerequisites for connecting to the C423 via Wi-Fi:

- You must be in close range to the C423 in order to connect to it via Wi-Fi — generally within 10 - 20 ft.
- A C423 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.

Change the 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 that the device's WebUI is not rendered unreachable.

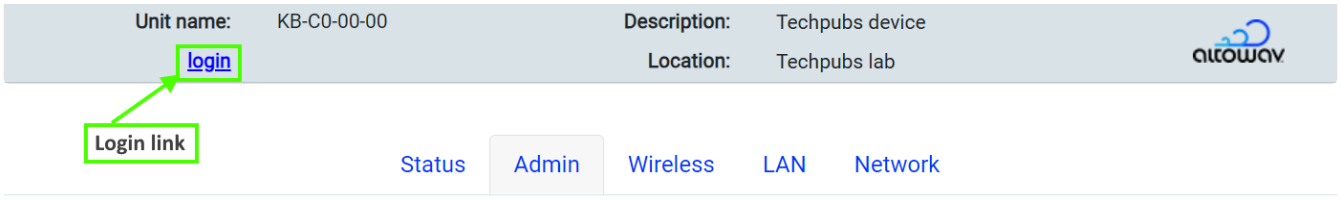
To change the device password:

1. Access the WebUI of the C423. In your browser's address bar, type:

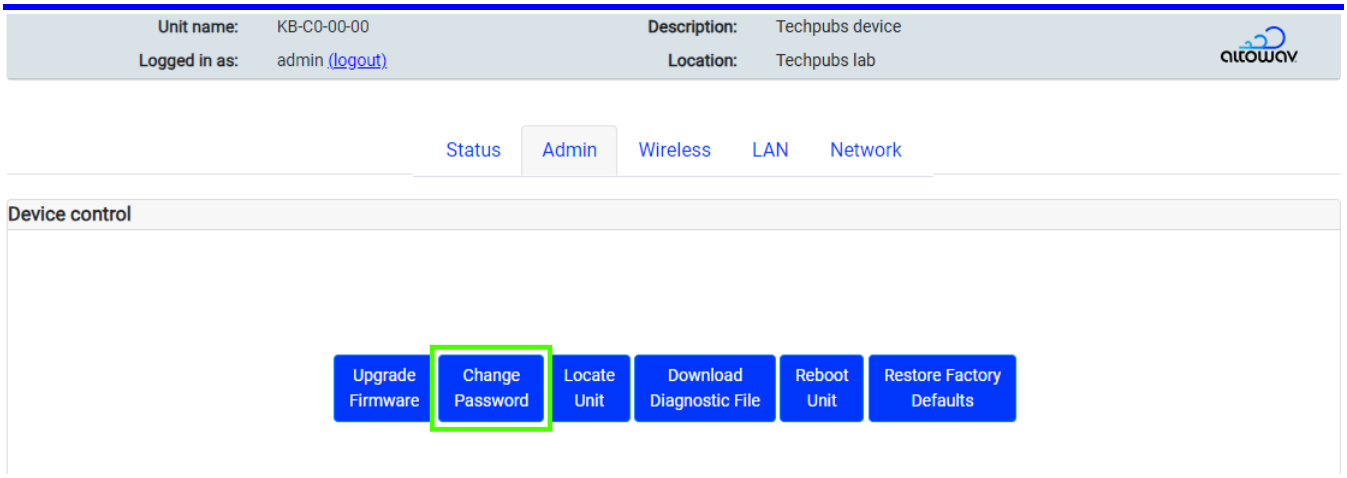
   https://*hostname*

   where *hostname* is the hostname (KB-XX-XX-XX) or IP address of the radio. See Connecting to the for more information.

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



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



The Change user password dialog opens.

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

Enable Passwordless SSH

By default, the C423 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 C423.

Note: This procedure describes how to upload an SSH key to the C423. You need to generate the SSH key on your local machine using a tool such as the Linux **ssh-keygen** command.

1. Log in via ssh to the C423:

   $ ssh admin@<*hostname*>

   admin@<*hostname*>'s password:

   where *hostname* is the hostname (for example, KB-C7-00-01) or IP address of the radio. See Connecting to the for more information.

2. Enter **control** mode:

   KB-C7-00-01> control

   KB-C7-00-01(control)>

3. 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.

Upgrading firmware

Upgrade roadmap

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

1. Download and unzip the firmware zip file from Altoplex Firmware Downloads at support.altowav.com.
2. Upgrade the devices one at a time.
3. Always start with the distribution node 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.
5. Upgrade client nodes after the distribution nodes are upgraded.

The firmware binary filename

The following files are included in the firmware zip file:

- A digest file, not used as part of this upgrade process.
- The firmware binary.

The firmware binary filename consists of three parts:

<filetype>-<device_family_name>-<version_number>

where:

- *filetype* is **kb_sw-prod**
- device_family_name is one of:
  - **NOMAD** — Firmware used for D621 devices.
  - **DEVO** — Firmware used for C423, C410, C420, and P421 devices.
- *version_number* is the version number of the firmware.

For example:

kb_sw-prod-DEVO-4.2.0

Upgrade from the WebUI

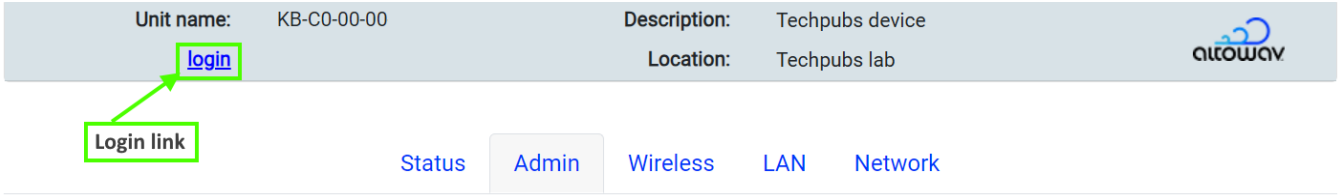
1. Download and unzip the firmware zip file from Altoplex Firmware Downloads at support.altowav.com.

   The following files are included in the firmware zip file:

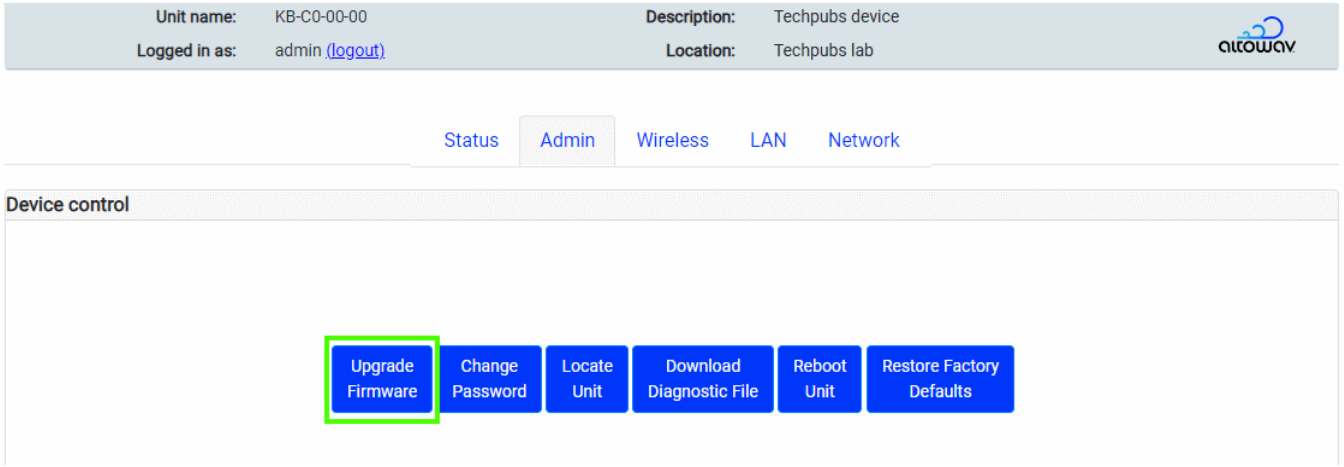
   - A digest file, not used as part of this upgrade process.
   - The firmware binary. See The upgrade software filename for information about the filename used for the firmware binary.
2. Access the WebUI of the C423. In your browser's address bar, type:

   https://*hostname*

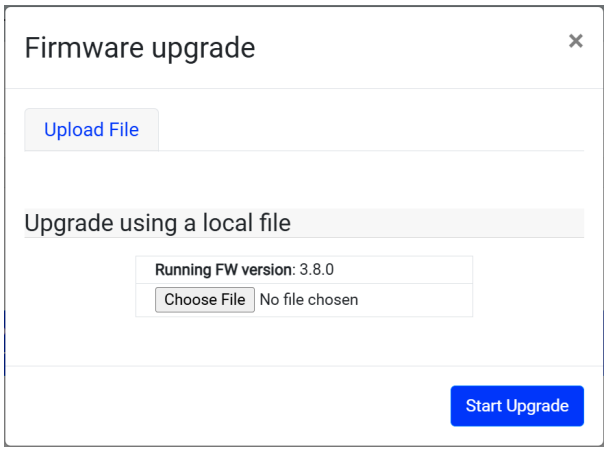
   where *hostname* is the hostname (KB-XX-XX-XX) or IP address of the radio. See Connecting to the for more information.
3. Click the **login** link in the WebUI header to log in as administrator. The default password is **admin**.



4. Click the **Admin** tab.
5. Click the **Upgrade Firmware** button.



The **Firmware upgrade** dialog opens.



6. Click Choose File.
7. Browse to the directory where the upgrade binary file was downloaded and select the file.
8. Click Start Upgrade.

Upgrade from the CLI

Upgrade from the CLI by using Secure File Copy (scp)

Use Secure File Copy (scp) to upload a file from a remote host to the C423 and install the file:

1. Download and unzip the firmware zip file from Altoplex Firmware Downloads at support.altowav.com.

   The following files are included in the firmware zip file:

   - A digest file, not used as part of this upgrade process.
   - The firmware binary. See The upgrade software filename for information about the filename used for the firmware binary.

2. Log in via ssh to the C423:

   $ ssh admin@<*hostname*>

   admin@<*hostname*>'s password:

   where *hostname* is the hostname (for example, KB-C7-00-01) or IP address of the radio. See Connecting to the C423 for more information.

3. Enter **control** mode:

   KB-C7-00-01> control

   KB-C7-00-01(control)>

4. Upload and install the software:

   KB-C7-00-01(control)> software upgrade scp://*user@server/firmware_filename*

   where:

   - *user* is the name of the user on the remote host.
   - *server* is the hostname or IP address of the remote host.
   - *firmware_filename* is the path and filename of the upgrade software.

5. When prompted, type the password to log into the remote host.

   The upgrade software will be uploaded and installed on the C423. You can monitor the status of the upgrade by using the **software status** command:

```
KB-C7-00-01(control)> software status
 current-software-version: 3.9.1
 status: upgrading
 running-sw-version: 3.9.1
 new-sw-version: 4.2.0
 upgrade-running: yes
```

After the software upgrade completes, the device will reboot.

Upgrade from the CLI by using a TFTP server

1. Download and unzip the firmware zip file from Altoplex Firmware Downloads at support.altowav.com.

   The following files are included in the firmware zip file:

   - A digest file, not used as part of this upgrade process.
   - The firmware binary. See The upgrade software filename for information about the filename used for the firmware binary.
2. Upload the binary file to the TFTP directory on your server. The TFTP server must be accessible from each device being upgraded.
3. Log in via ssh to the C423:

   $ ssh admin@<*hostname*>

   admin@<*hostname*>'s password:

   where *hostname* is the hostname (for example, KB-C7-00-01) or IP address of the radio. See Connecting to the for more information.
4. Enter **control** mode:

   KB-C7-00-01> control

   KB-C7-00-01(control)>
5. Upload and install the software:

   KB-C7-00-01(control)> software upgrade tftp://*server*/*firmware_filename*

   where:

   - *server* is the hostname or IP address of the TFTP server.
   - *firmware_filename* is the path and filename of the upgrade software.

   The upgrade software will be uploaded and installed on the C423. You can monitor the status of the upgrade by using the **software status** command:

```
KB-C7-00-01(control)> software status
 current-software-version: 3.9.1
 status: upgrading
 running-sw-version: 3.9.1
 new-sw-version: 4.2.0
 upgrade-running: yes
```

After the software upgrade completes, the device will reboot.

Upgrade from the REST API

1. Download and unzip the firmware zip file from Altoplex Firmware Downloads at support.altowav.com.

   The following files are included in the firmware zip file:

   - A digest file, not used as part of this upgrade process.
   - The firmware binary. See The upgrade software filename for information about the filename used for the firmware binary.
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 -u admin:<*password*> \
   https://<*hostname*>/rest/v002/configuration/software_upgrade \
   -X POST \
   -H "Content-Type:application/octet-stream" \
   -H "X-File-Name:<*filename*>" \
   --data-binary@<*path*>/<*filename*>

   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-4.2.0.
   - *hostname* is the hostname or IP address of the radio 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-4.2.0.plain" \

   --data-binary @kb_sw-prod-DEVO-4.2.0.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 2025 00:23:39 GMT

Server: lighttpd/1.4.73

{

"status":"starting",

"running-sw-version":"3.9.1",

"upgrade-running":"yes"

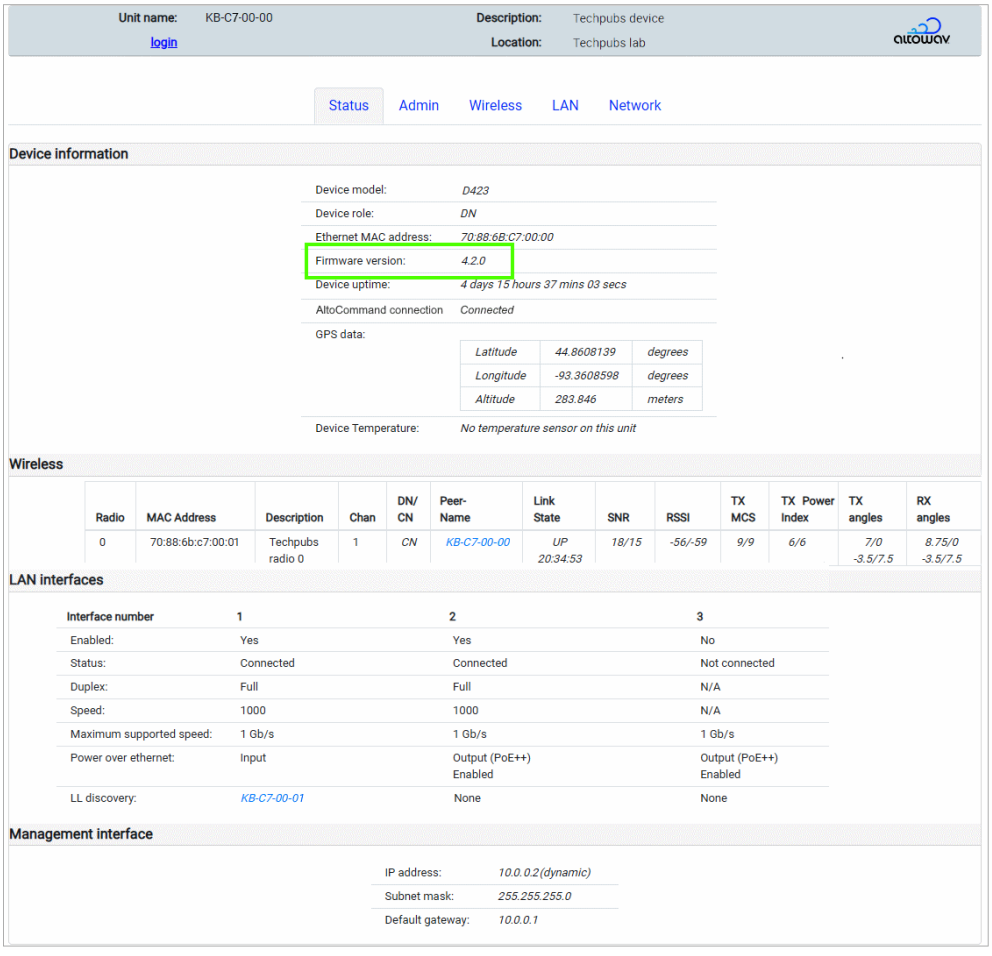
}

The upgrade may take up to several minutes to complete.

Verify that the firmware update was successful

Verify firmware update from the WebUI

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



Verify firmware update from the command line

1. Log in via ssh to the C423:

   $ ssh admin@<*hostname*>

   admin@<*hostname*>'s password:

   where *hostname* is the hostname (for example, KB-C7-00-01) or IP address of the radio. See Connecting to the for more information.

2. Enter **control** mode:

   KB-C7-00-01> control

   KB-C7-00-01(control)>

3. Check the status of the device by using the **software status** command:

   KB-C7-00-01(control)> software status
   current-software-version: 4.2.0
   status: idle
   upgrade-running: no

   KB-C7-00-01(control)>

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

Verify firmware update from the REST API

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

```
$ curl -k -u admin:admin https://KB-C7-00-01/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:C7:00:01",
  "HW name" : "devo",
  "HW rev" : 2,
  "HW type code" : 82,
  "Node role" : "CN",
  "Number Ethernet Interfaces" : 1,
  "Number RF Interfaces" : 1,
  "Part number" : "1900-8411-1012-devo-2-LBKA0ZZ1SV1",
  "Serial number" : "00000000000000000001KB-C7-00-01:2",
  "authorized_org" : "",
  "bootloader version" : "KBBLVERSION:1.3:prod:robot:2025-12-04_11-57-10:devo:1b565eb",
  "description" : "system description not set",
  "gps available" : 1,
  "location" : "system location not set",
  "name" : "KB-C7-00-01",
  "node type" : "PTP",
```

"software" : "4.2.0"
}

Reboot a device

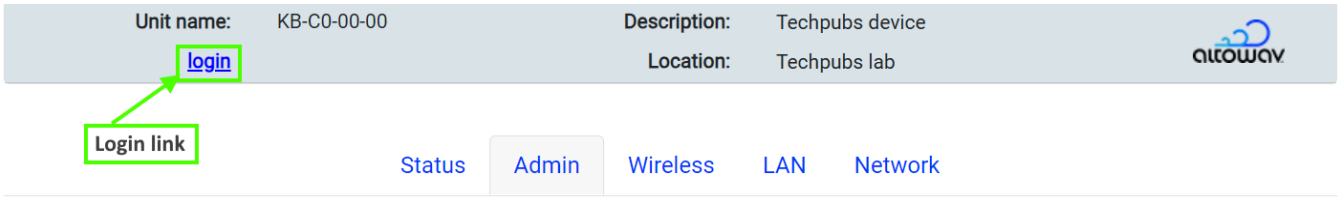
Note: A power-cycle or reboot clears the diagnostic log information stored in the device. So during troubleshooting, you should capture the diagnostic log in a file, before the power-cycle or reboot. If you require troubleshooting assistance, information in the diagnostic log may be useful.

1. Access the WebUI of the C423. In your browser's address bar, type:

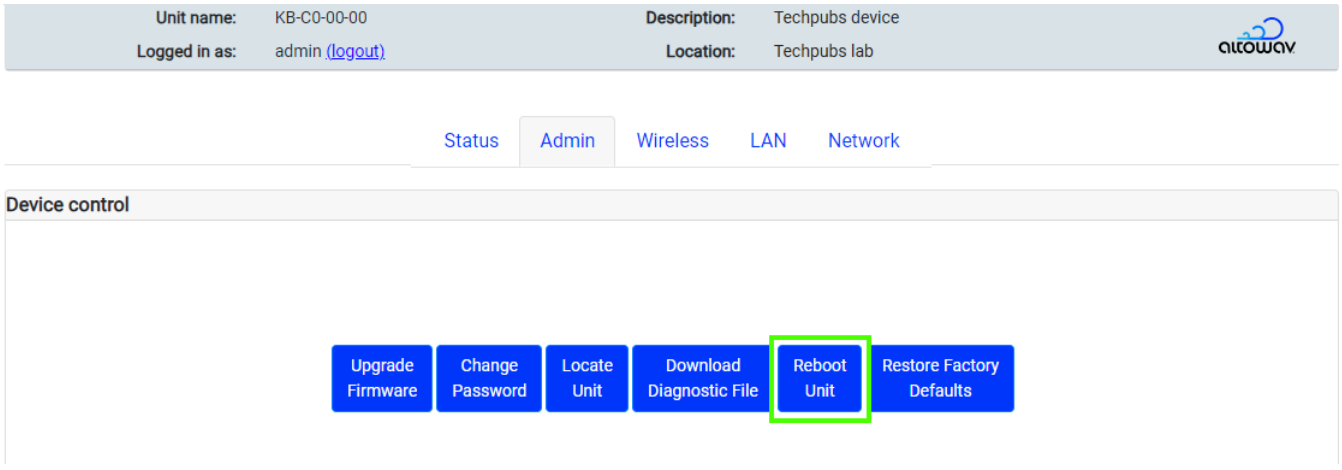
   https://*hostname*

   where *hostname* is the hostname (KB-XX-XX-XX) or IP address of the radio. See Connecting to the for more information.

2. Click the **login** link in the WebUI header to log in as administrator. 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.



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

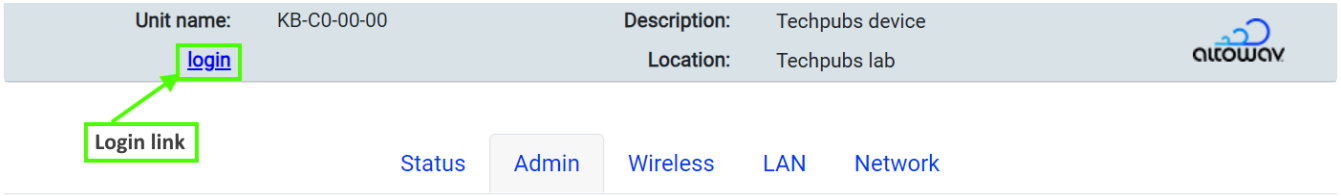
Use the **Restore Factory Defaults** button in the device's WebUI to reset the device.

1. Access the WebUI of the C423. In your browser's address bar, type:

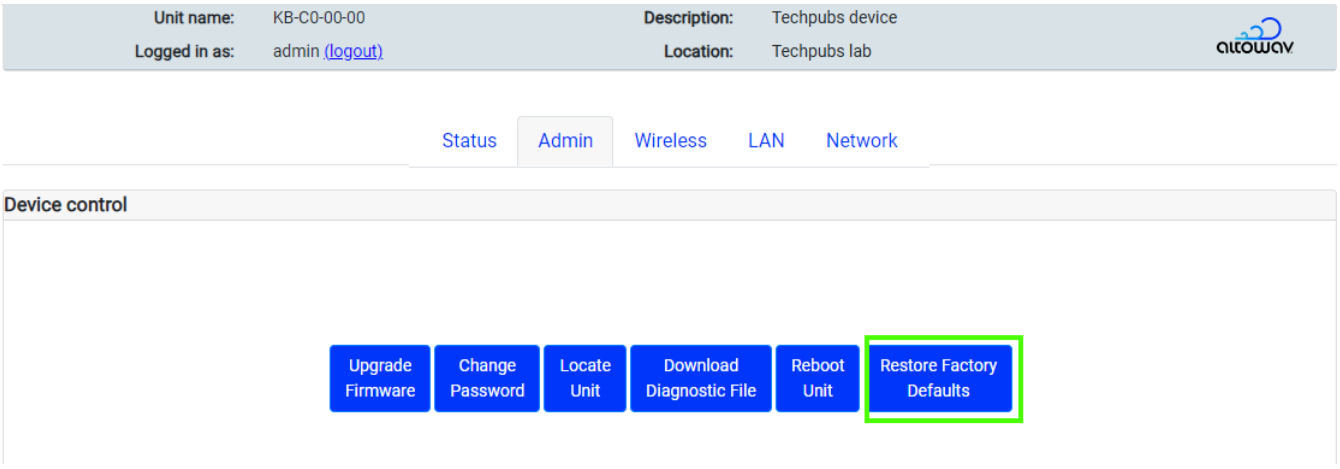
   https://*hostname*

   where *hostname* is the hostname (KB-XX-XX-XX) or IP address of the radio. See Connecting to the for more information.

2. Click the **login** link in the WebUI header to log in as administrator. 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.



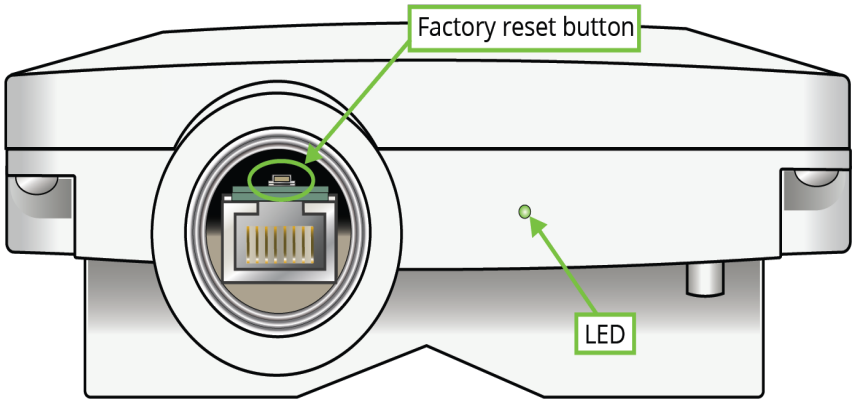
5. A confirmation dialog opens. Enter the text **confirm factory reset** and click **OK**.

After the reset, the device reboots with factory default settings. The login credentials for the device return to **admin**. Reconfigure the device as necessary to reestablish radio links, set location and description, and configure the network settings.

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.

1. To access to the reset button, the Ethernet port on the device must be uncovered. If the cable gland is in place, unscrew or remove the gland.



2. Reboot or power cycle the device.
    - While the device is powering up, The LED will be solid red.
    - After powering up, the the LED will begin flashing red/green, pausing, then flashing red/green again.

This indicates that the device is 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.

3. Insert a wood or plastic pin into the factory reset button above the RJ45 port. Push down and hold.
4. Continue to hold the reset button down until the LED flashes a red and green sequence, then release the button.
5. The LED is solid red while the device boots.
6. When the LED flashes green, the reset is complete.

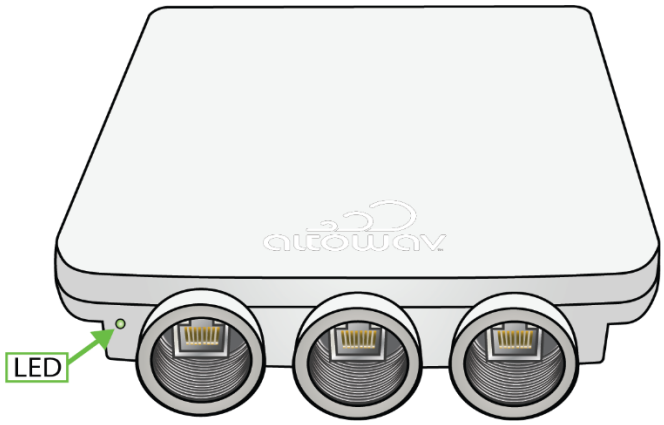
After the reset, the device reboots with factory default settings. The login credentials for the device return to **admin**. Reconfigure the device as necessary to reestablish radio links, set location and description, and configure the network settings.

Troubleshooting

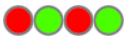
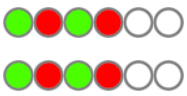
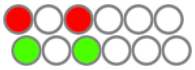
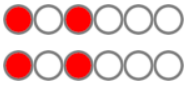
This chapter contains the following topics:

LED Indicators

The C423 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.
	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 C423 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.

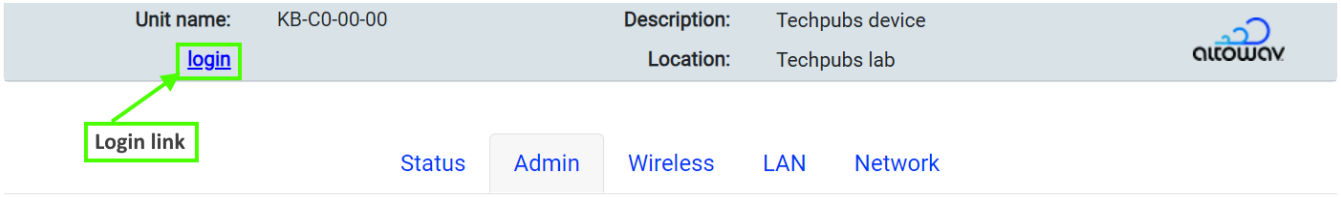
Follow these steps to download a diagnostic file for connected devices from the WebUI:

1. Access the WebUI of the C423. In your browser's address bar, type:

   https://*hostname*

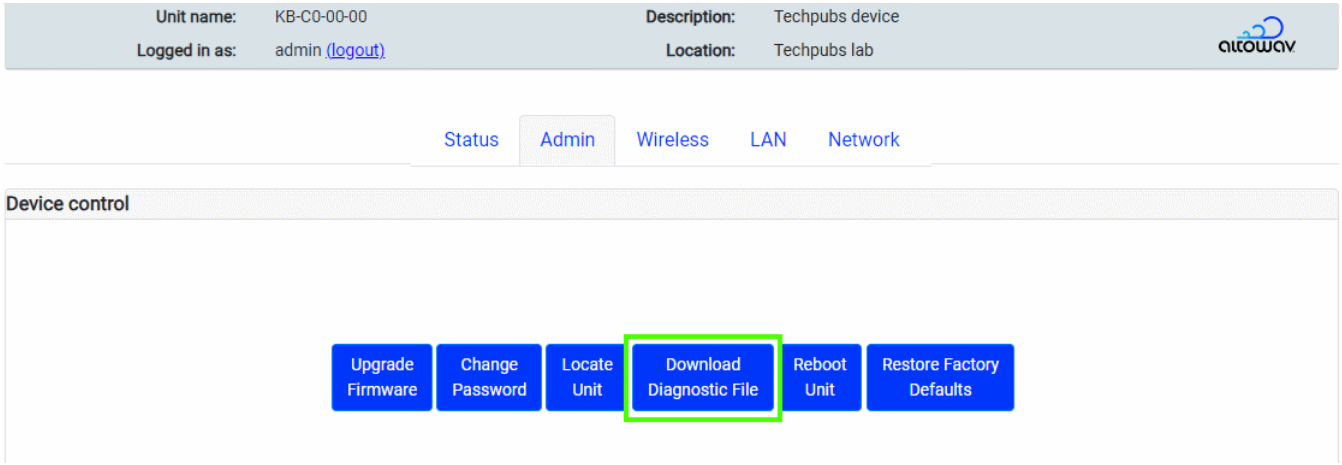
   where *hostname* is the hostname (KB-XX-XX-XX) or IP address of the radio. See Connecting to the for more information.

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



3. Click on the **Admin** tab.

4. Click on the Download Diagnostic File button in the Device control section.



5. 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-C7-00-01_diag_2025-12-04-20-32-26.txt
6. 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.

MAC addresses used by the C423

AltoPlex devices have several interfaces that are each assigned unique MAC addresses. These MAC addresses may appear in packet capture software, DHCP server logs, and the device's diagnostic file.

Interface	Description		Example MAC address
60 GHz wireless radio (wlan0)	The MAC address on the device label. The wlan0 interface is also known as Radio 0.		70:88:6B:C7:00:00
Bridge (br0)	Administratively assigned MAC address for the bridge interface. The br0 interface uses the same MAC address as wlan0, except the first octet is 72 rather than 70.		72:88:6B:C7:00:00
eth1	Ethernet port 1	The eth* interfaces use the same MAC address as wlan0, except sequentially incremented by one.	70:88:6B:C7:00:01
eth2	Ethernet port 2		70:88:6B:C7:00:02
eth3	Ethernet port 3		70:88:6B:C7:00:03

Note: The device's diagnostic file also contains interfaces that are named kb0* and terra*. These interfaces and their corresponding MAC addresses are for internal use and can be ignored.

Glossary

802.11ay — An enhanced standard for WLANs operating in the 60 GHz spectrum.

Backhaul — Networking infrastructure that connects a local subnetwork to the primary network. Also known as network backhaul.

Channel — In Wi-Fi networking, a channel is a specific frequency range within a broader range. The radios in AltoPlex devices can be configured to operate on one of four channels within the 60 GHz spectrum.

Client node — A node that acts as a client to a distribution node. Client nodes connect to one distribution node. Distribution nodes can connect to up to fifteen client nodes.

CN — See Client node.

CN link — A link between a distribution node and a client node. Sometimes referred to as a DN-CN link.

CN responder — In a CN link, the CN responder is the client node that accepts the DN initiator's link.

Device hostname — In AltoPlex devices, the device hostname uses the last three octets of the device's MAC address, with **KB** appended to the beginning. For example, KB-C7-00-01.

Distribution node — Distribution nodes serve as connected nodes in a distribution network. Distributions nodes can provide network access via a wired connection to the backhaul network, wired connections through a switch to other distribution nodes, and wireless connections to other distribution nodes and to _rh_pdf_topic_id_19-client-nod.

DN — See _rh_pdf_topic_id_19-distributi.

DN link — A link between two distribution nodes. Distribution nodes can be linked together in a point-to-point, hub-and-spoke, or ring topology.

DN responder — In a DN link, the DN responder is the DN device that accepts the DN initiator's link. See also responder.

Fixed wirelesss access — Networking technology that provides high-speed network access to a fixed location using a radio connection.

FWA — See Fixed wireless network.

GPON — Gigabit Passive Optical Network. A high-bandwidth mechanism for providing network access to a fibre optic backhaul network.

Golay index — An error correction mechanism used in wireless communications to mitigate co-channel interference. Wireless devices communicating on the same channel can mitigate interference by using different Golay indexes.

Hub-and-spoke — A network topology that involves central nodes with access to the backhaul network, and several nodes wirelessly connected to those central nodes.

Initiator — The _rh_pdf_topic_id_19-distributi that initially establishes a link with a remote device. By default, the intiator is the radio interface with the lower MAC address. See also responder.

MCS — Modulation Coding Scheme. AltoPlex devices use a weighted MCS value of 2-12. MCS is prioritized in AltoPlex devices. MCS and TX power are adjusted automatically based on Power/packet Error Rate (PER). A link will stay at MCS 9 when minimal network traffic is observed.

Node — A single AltoPlex device in a multi-device installation.

NTP — Network Time Protocol. Enables the synchronization of a device's time to an upstream NTP server.

Point-to-point — A network topology in which two devices are directly connected to each other.

Point-to-multipoint — A network topology in which multiple devices are connected to a central node. In a point-to-multipoint network, AltoPlex distribution nodes support one DN link and up to fifteen CN links.

Polarity — Polarity is a mechanism of TDMA used in determining when to transmit or receive during a timing cycle. Polarity is either odd or even.

P2P, **PtP** — See point-to-point.

PtMP, PMP — See point-to-multipoint.

Point of presence — The location or facility that connects to the Internet. Often this may be an equipment cabinet or similar location with fiber access to the primary network and/or the internet.

PoP — See point of presence.

PoP node — The distribution node (or nodes) that is directly connected to the primary network and/or the internet. This distinction is important for optimizing traffic when designing network topology. During deployment, the PoP node devices are the first installed. During firmware upgrades, they are typically the last upgraded.

Rebeamform — A process by which a low-performing wireless connection between two AltoPlex devices is replaced with another wireless connection.

Responder — An AltoPlex device that does not initially establish a link with another device, but instead responds a link initiation request from an initiator device. By default, the responder is the radio interface with the higher MAC address. This information may be useful for network design, and in rare cases during troubleshooting after a power outage.

Ring topology — A network topology in which devices are connected in a circular closed loop.

RSSI — Received Signal Strength Indicator. A measurement of how well a device can receive signals from external wireless devices.

SNMP — Simple Network Management Protocol. Used to monitor and report on all the devices in your network.

TDMA — Time Division Multiple Access, used with GPS synchronization for timing in AltoPlex devices.

TX power — Transmission power. Determines how powerful a transmitted signal is.