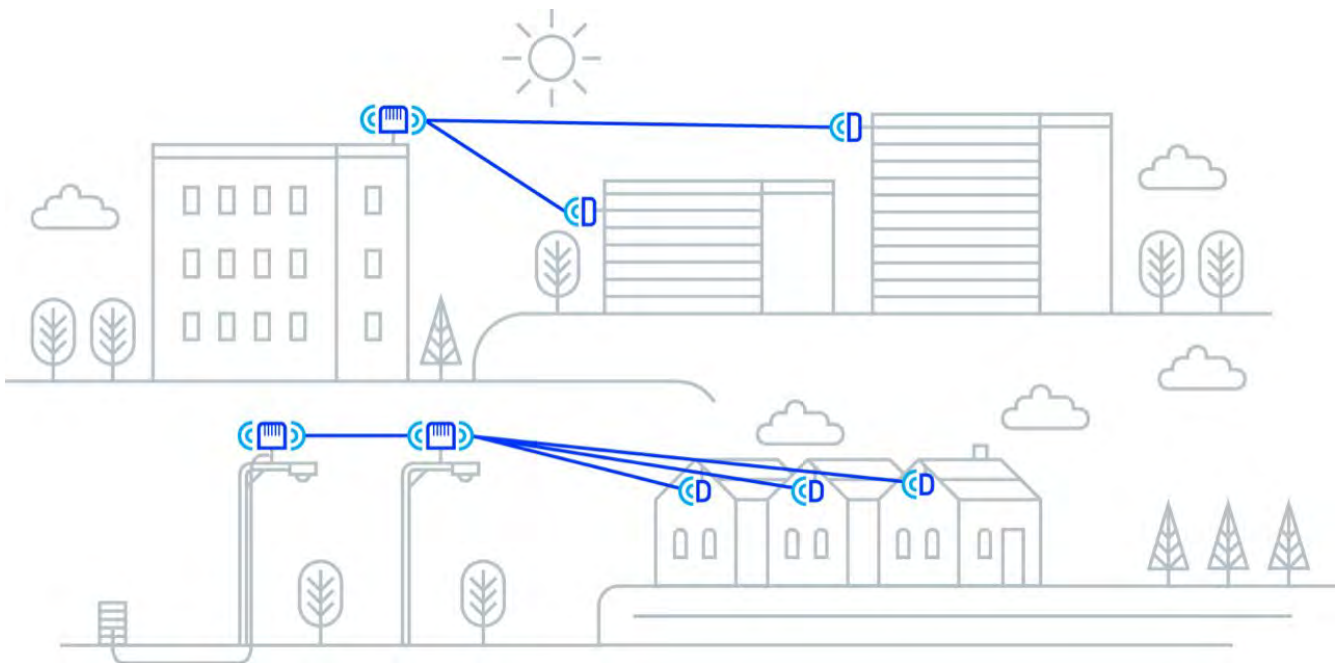




Altoway AltoPlex Series D423 User Guide

Version 4.2.0
December 4, 2025

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 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 D423.

© 2025 Altowav Inc. All rights reserved.

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.

Regulatory statements**FCC Radiation Exposure Statement**

The D423 device complies with FCC radiation exposure limits set forth for an uncontrolled environment. A minimum of 35 centimeters (14 inches) of separation between the D423 and all persons shall be maintained.

FCC Regulatory Statement

The D423 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 D423 device complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. A minimum of 35 centimeters of separation between the D423 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 D423 et toutes les personnes doit être maintenu.

ISED Industry Canada Regulatory Statement

The D423 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 licence qui sont conformes aux CNR exempts de licence d'Innovation, Sciences et Développement économique Canada. Son fonctionnement est soumis aux deux 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 indésirable 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 D423:

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
Updated for the 4.2.0 software release: • Added information about changing the SSID and encryption passkey for the 60 GHz airlink. • Added description of the new Link State parameter in the Wireless table on the Status tab, and the Wireless Status table on the Wireless tab, of the WebUI. • Added information about a new Hide SSID configuration parameter that hides the diagnostic Wi-Fi SSID.	12/04/2025
Initial release of the D423.	xx/xx/2025

Contents

D423 User Guide overview	7
Additional Documents	7
Additional help	7
Introduction — The AltoPlex platform.....	8
D423 Installation and Configuration	9
Network topology design and deployment.....	9
Preparing for installation	18
Connecting to the D423	23
Installation.....	26
Configuration	29
Maintenance and security	61
Wi-Fi connection to a D423	61
Change the device password.....	63
Enable Passwordless SSH	64
Upgrading firmware.....	65
Reboot a device	72
Factory reset	73
Troubleshooting.....	75
LED Indicators.....	76
Lost Password.....	78
Download a Diagnostic File.....	78
MAC addresses used by the D423.....	80
Glossary.....	81

D423 User Guide overview

Thank you for choosing the Altowav AltoPlex series for your fixed-point networking solution. This user guide describes installation, configuration and operations of D423 devices.

This guide is intended for network and system administrators who will install, configure, and manage Altowav networks using D423 devices.

This guide includes instructions for the installation, configuration and management of D423 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 D423 devices:

- For general technology specifications and product datasheets, see altowav.com/technology/
- [D423 Quick Start Guide](#)
- [C410 and C420 Quick Start Guide](#)
- [C410 and C420 User Guide](#)
- [Altowav AltoCommand User Guide](#)
- The AltoPlex series 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 — The AltoPlex platform

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.

D423 Installation and Configuration

Network topology design and deployment

The D423 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 D423 is designed to operate as either a distribution node or a client node, and with the D621, C410, C420, and with previous AltoPlex devices (model numbers K60DN and K60CN1).

About AltoPlex wireless links

- 60GHz wireless links rely on clear line of sight (LOS).
- Device roles: D423s may be configured as distribution nodes (DNs) for distribution, or as client nodes (CNs) used for client access.
- Priorities:

These general guidelines may vary depending upon specific network topology. Keep your specific network requirements in mind.

- When planning, designing, and deploying your network, give priority to the distribution nodes to benefit the entire network. Devices closest to the point of presence (PoP) will have the heaviest traffic.
- Links between distribution nodes are often built first to facilitate throughput, starting at the PoP.

- Links between distribution nodes and client nodes are often added after distribution node links are up and running.
- Consider the distribution and density of clients during the design and planning of networks. Up to fifteen clients can link to one distribution node. However, dense environments are likely to have more interference, and linking clients to different distribution nodes allows you to manage interference among dense client networks by using different channels.
- Configure D423 wireless links to other units through WebUI settings.
 - Links between distribution nodes can be configured after installation in the field by using the [DN link auto-configuration](#) feature. They can also be configured manually, generally by using [bench configuration](#) prior to installation, by setting the **DN responder** link on each distribution node.
 - Links between distribution nodes and client nodes are [configured on the distribution node](#) in the **CN responder** list setting. This is typically done as clients are installed.
- Weighted MCS levels are a good performance metric for the AltoPlex products. Power control in the D423 adjusts automatically to drive optimal MCS levels.

D423 — General information

Use this information to determine how best to fit the D423 into your specific network design.

Capacity/throughput: 2 Gbps Aggregate

Range: Expected maximum range for a D423-to-D423 link: Up to 1,312 feet (400 meters).

Ethernet: Three 1.0 Gbps RJ45 ports:

- Port 1: PoE input, 90W maximum.
- Ports 2 and 3: PoE output:
 - 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.

Role: The D423 can be configured as a distribution node for distribution or as a client node to serve as a multiport client device.

Scan range: 90° azimuth (-45° to 45°) for a single wireless sector. 40° elevation range. Mounting hardware provides additional aiming flexibility.

Forming DN links with the D423: The [DN link auto-configuration](#) will configure DN-to-DN links, including:

- Automatically configure the DN responder with the correct link to the DN initiator.
- Automatically set the channel, Golay index, and polarity to the correct values.

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.

Forming CN links with the D423: The client node is added to the **CN Responder** list in the distribution node's WebUI, on the **Wireless** tab.

Maximum DN-to-DN links: 1 per radio interface.

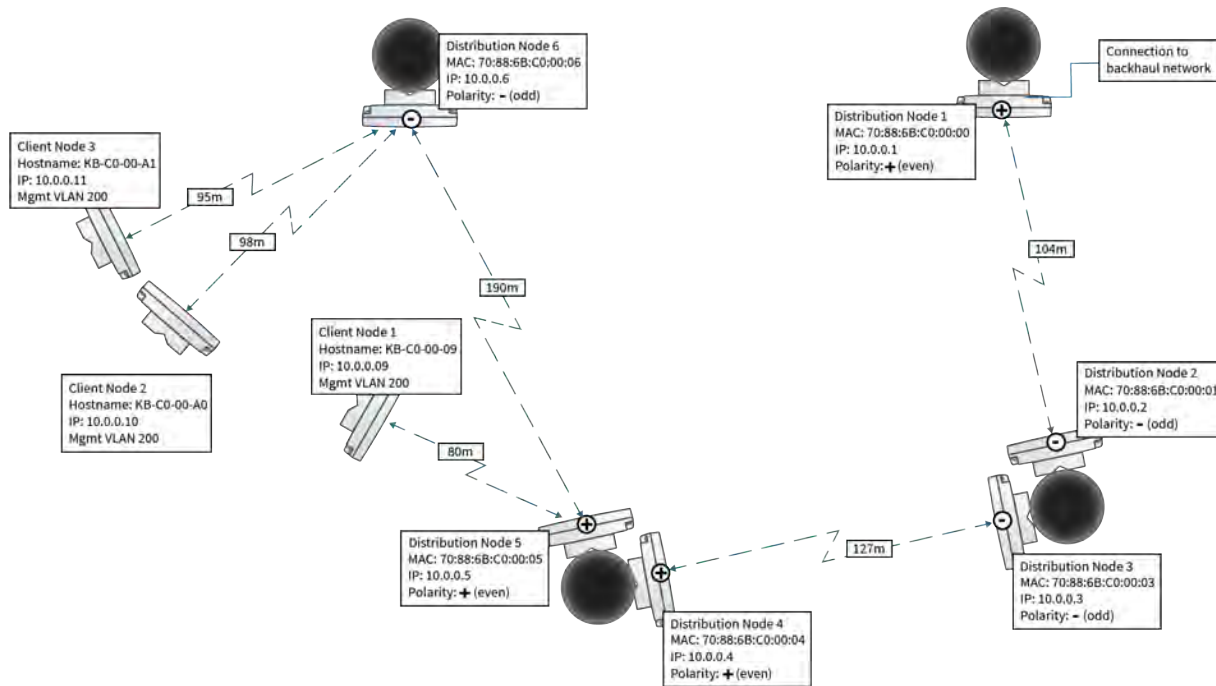
Maximum DN-to-CN links: 15 client node links per distribution node. A client node may have only link to only one distribution node.

GPS: Used for location and synchronization.

Wi-Fi management: A [Wi-Fi access point](#) is enabled by default for management and diagnostic purposes. The AP provides access to the radio only; it does not provide network or internet access.

Deployment for common topologies

Altoway recommends creating a detailed network design and deployment plan with specific device, network and location information. The following example is a general illustration of a network design plan; your specific situation will vary. Channel and golay code settings should be selected based on the deployment specifics; see [Design Issues to Avoid](#) for details about using channel and golay code settings.



Considerations for all deployments:

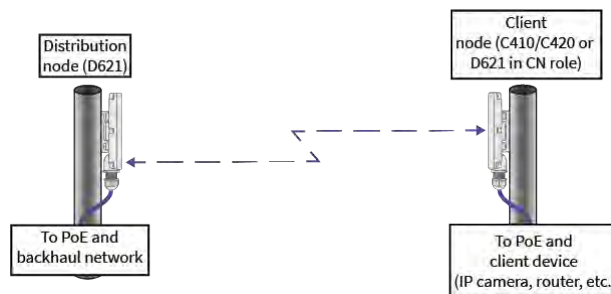
- Generally, all DNs on the same pole should have the same polarity. If your network requires opposite polarities on the same pole, make sure that the devices are set to different channels.
- Keep in mind performance and operational characteristics of the D423 for range, and throughput, as listed above.
- Follow [Installation](#) guidelines.
- Each D423 supports one DN link and up to 15 CN links.

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. Select the best role for each end of the link, according to its planned function in the network. At least one D423 in the PtP link must be configured as a distribution node.

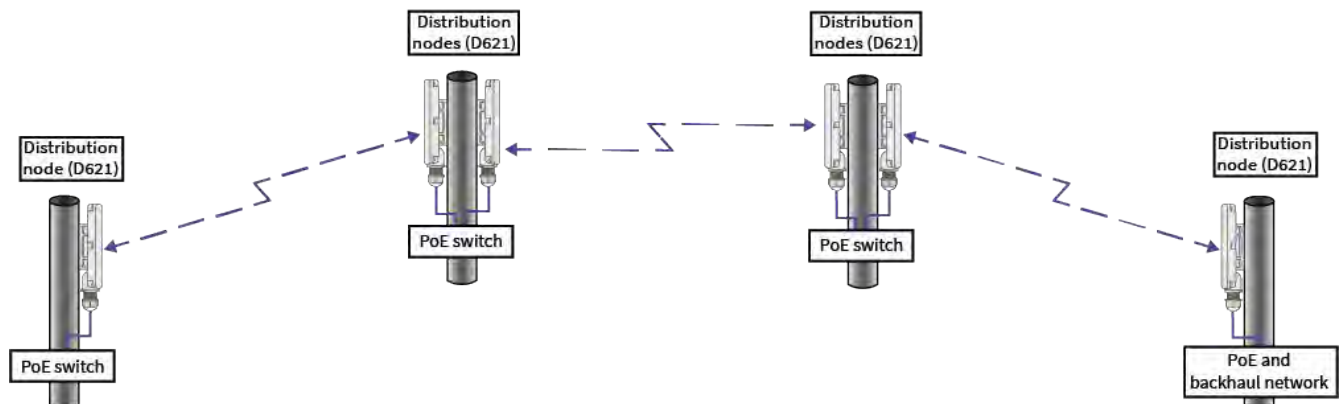
Point-to-point topology involving distribution node linked to a client node

The following diagram demonstrates a simple point-to-point topology.



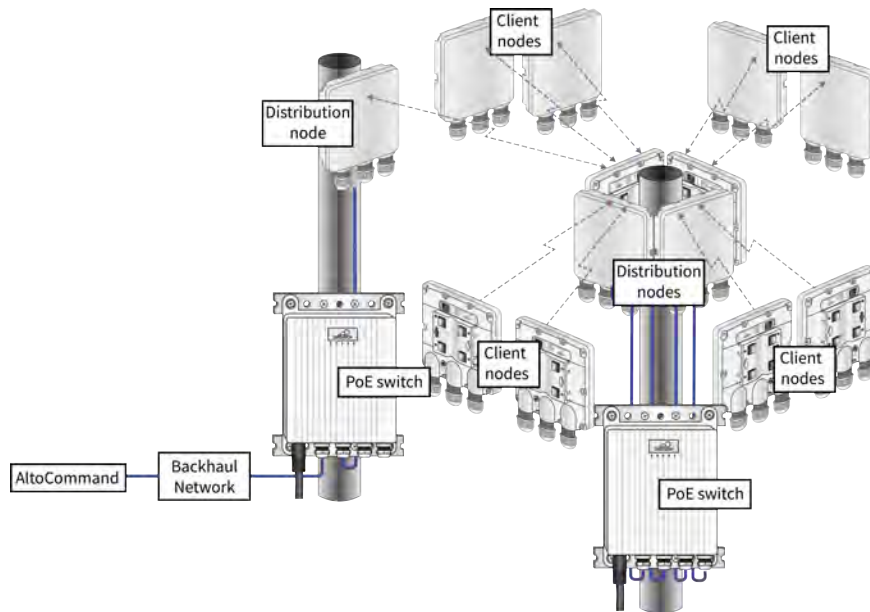
Point-to-point topology with multiple distribution nodes (daisy-chain)

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



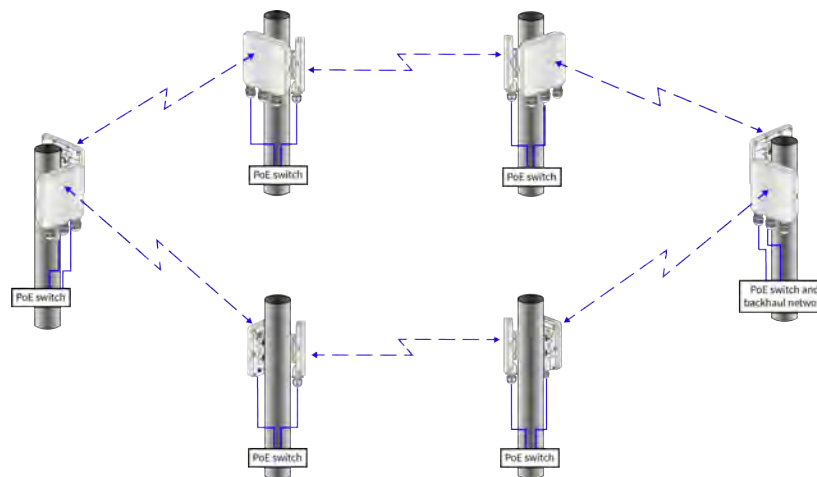
Point-to-multipoint deployment

In point-to-multipoint deployments, one distribution node wirelessly connects the backhaul network to distribution nodes networked via a switch.



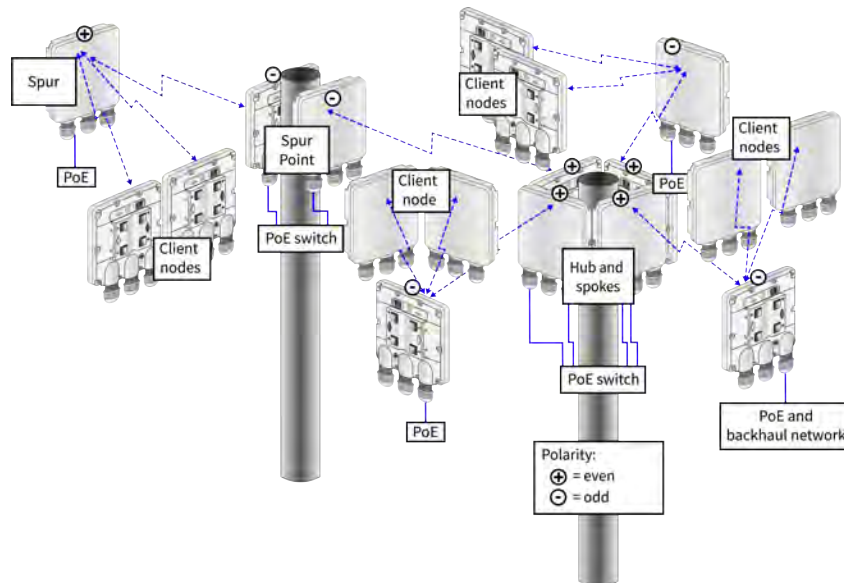
Ring deployment

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 (RSTP). RSTP should be enabled for ring topologies. RSTP is enabled by default on the D423 and disabled by default on dedicated client nodes (C410 and C420).



Spur or Spoke Deployment

A spur or spoke deployment extends the reach of a distribution network. At least two D423s are required at the spur switch point that extends distribution to a wider azimuth range.



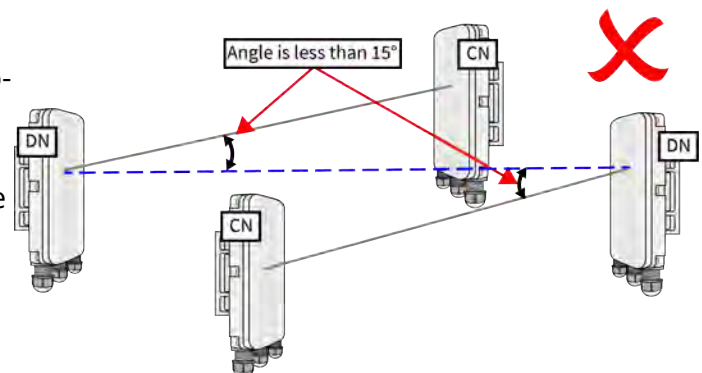
Design Issues to Avoid

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

Issue: Tight angles between DN links and CN links

Tight angles between the DN link and the CN link in the same sector, such as the butterfly topology, can result in early weak interference.

This problem occurs at angles tighter than 15°. Early weak interference can be hard to detect because it does not create any signal-to-interference-plus-noise ratio (SINR) degradation, but it still blocks desired packets by locking the receiver before the arrival of the packet.



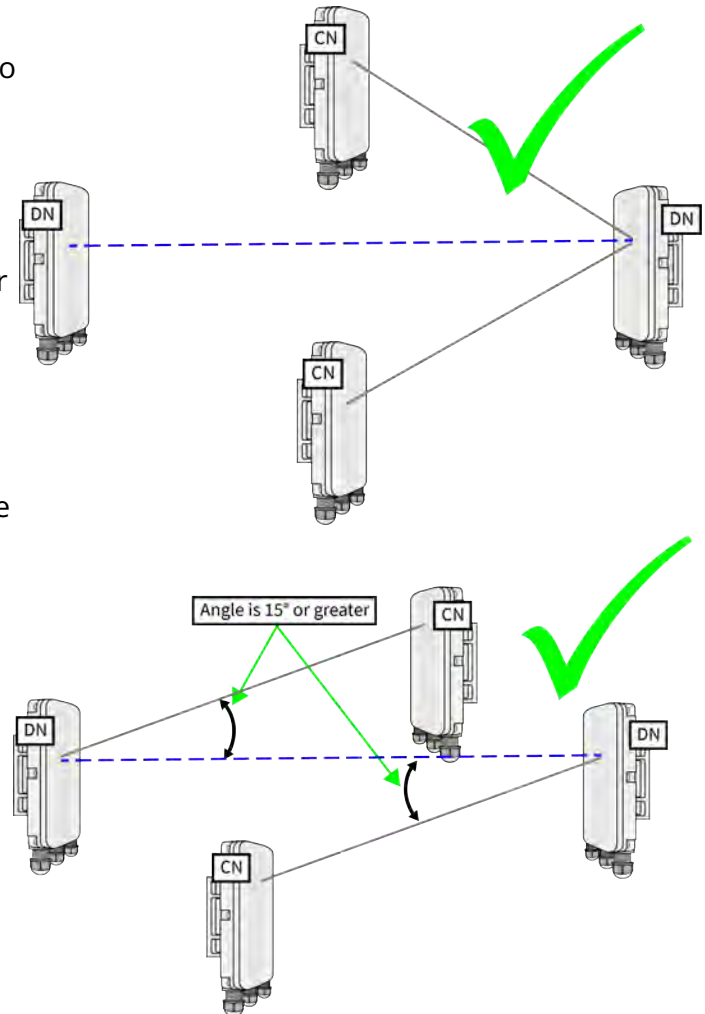
Best Practice:

If the client nodes cannot be positioned to avoid the tight angle, the best workaround is to link both client nodes to same distribution node.

Ideally the client nodes would link to the distribution node closest to the point of presence (PoP). This will minimize the number of hops from the PoP to the client node. This ideal is not always practical, due to site conditions and line of sight.

Additional Solution:

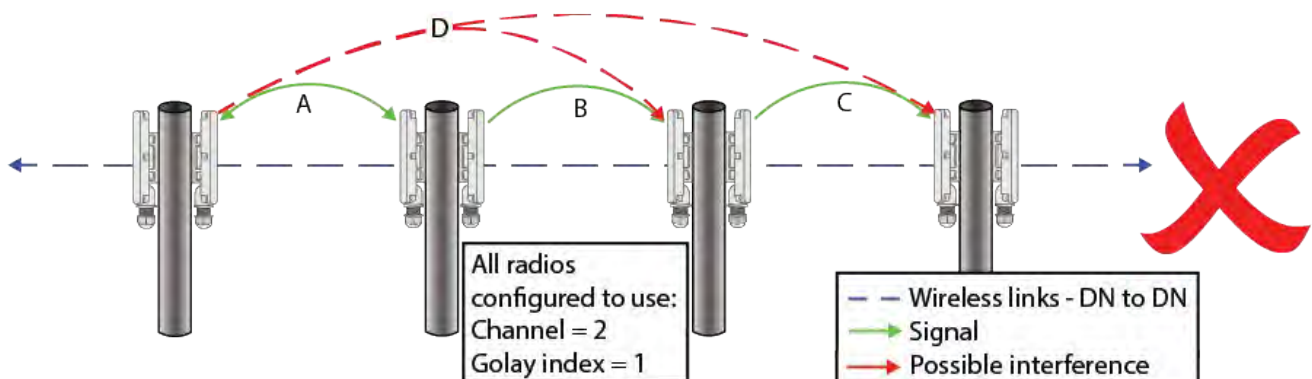
Design and deploy sites where the CN links are more than 15° away from the DN links as shown in the butterfly topology diagram below.



Issue: Distribution nodes in a straight line and close together

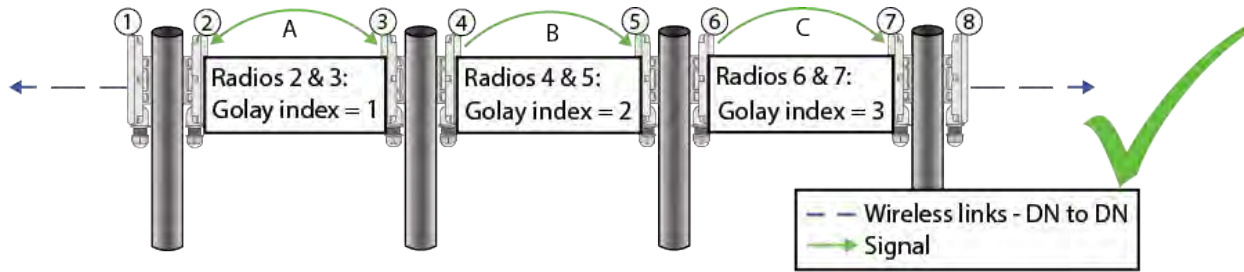
When three or more DN links are in a line and are using the same channel and golay code, a signal can be far reaching and cause interference to an unintended endpoint. Straight line interference is more impactful for short link distances.

The diagram below shows transmission using the same channel and golay index. In this case, signal A can also cause a signal D that may interfere with an unintended endpoint.

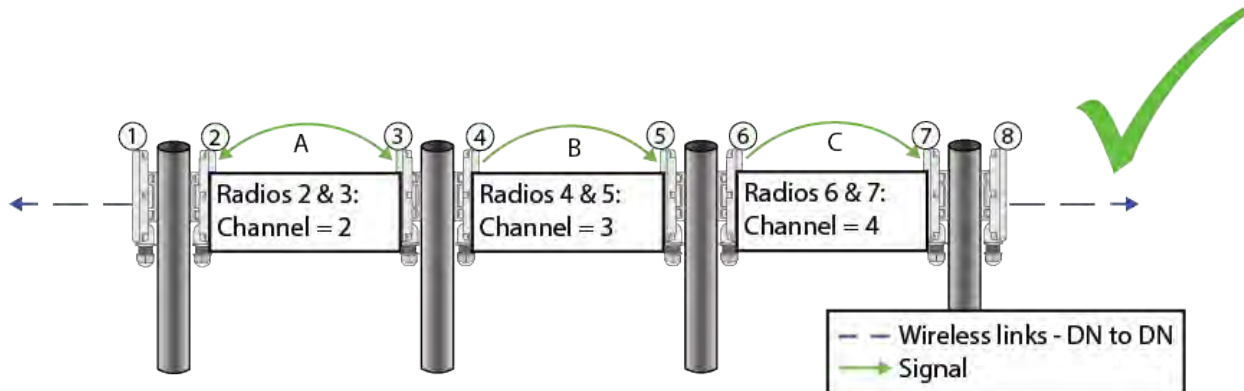


Solutions:

- **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.



- **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.



Preparing for installation

The D423 installation instructions include:

- Box contents and mounting options.
- Functional description.
- Network design information required.
- Bench configuration steps.
- D423 on-site installation steps.

Box contents

- D423 device.
- IP67 cable gland.
- QR code card for D423 Quick Start and D423 User Guide.
- Also available:
 - Wall Mount
 - Model number: AX-AW3-MT-WALL
 - Extended Range Pole Mount
 - Model number: AX-AW3-MT-EXT



About the D423

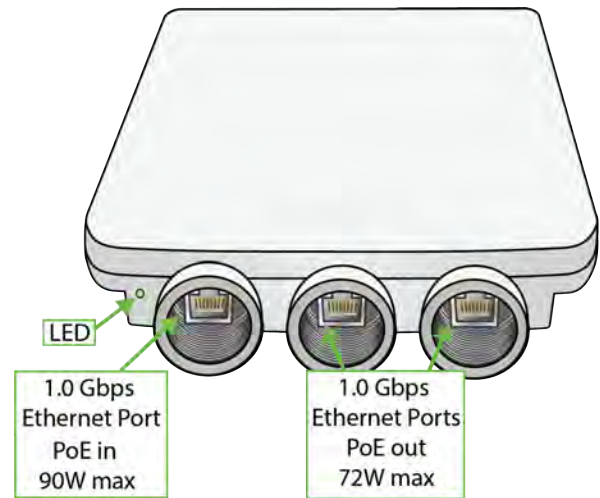
The D423 supports the AltoPlex series for 60 GHz wireless networks and provides wireless coverage for a 90° sector. See the for specifications and features. See [Design and Deployment](#) for general design and deployment information, best practices and considerations based on network topology.

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 D423 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.



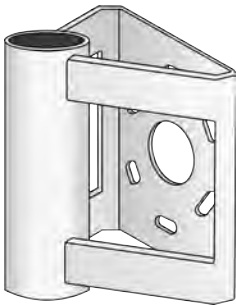
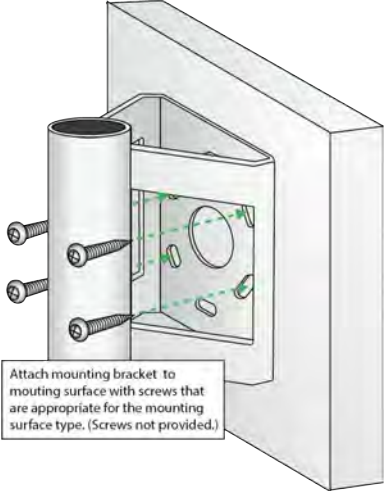
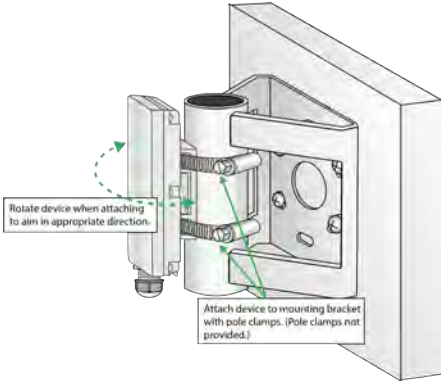
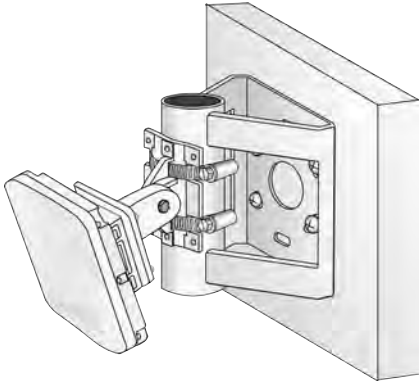
Mounting brackets

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

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

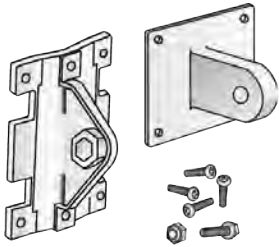
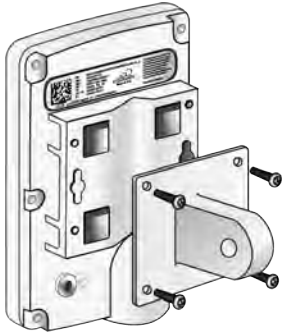
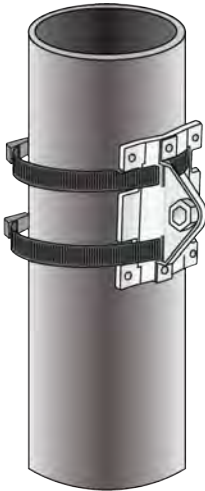
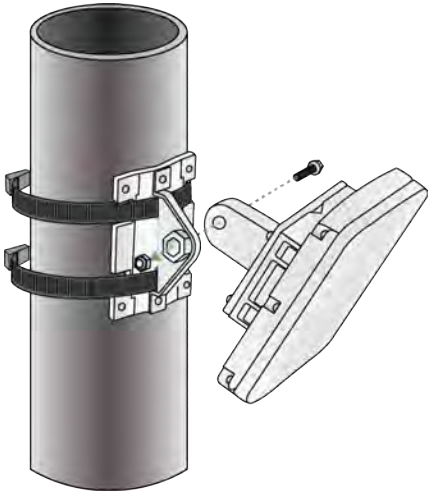
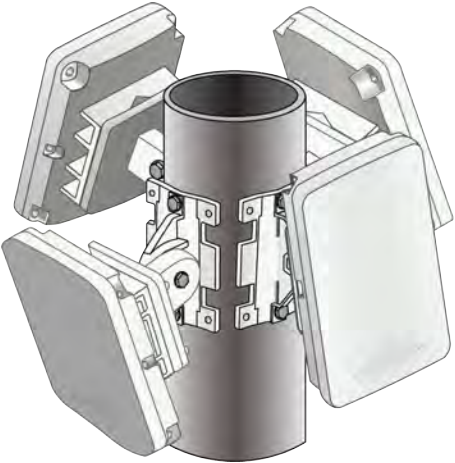
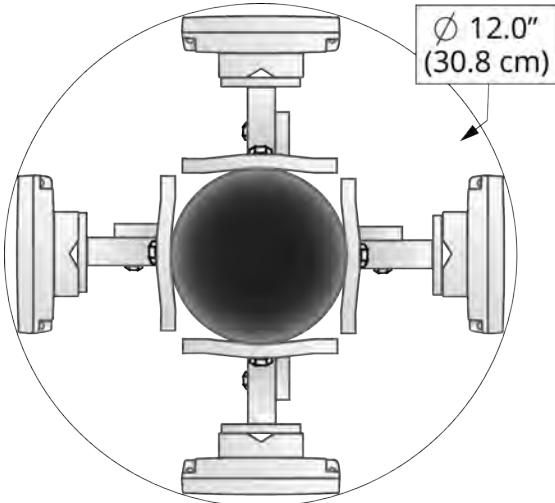
Altoway Wall Mount

The Altoway Wall Mount, model number AX-AW3-MT-WALL, can be used to securely mount the D423 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 D423 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 Altoway Wall Mount, as show above.

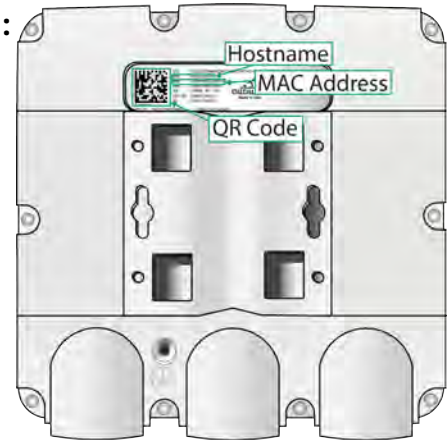
Bracket	Attach to the D423
	
Pole mounting with band clamps	
	
360° coverage	Small form factor
	

Required network design information

Note: The terms DN and CN are used to describe the role of a device: distribution node or client node. D423 devices can operate in DN role, and can also operate as multi-port CNs. The role for a D423 is configured on the [Wireless tab](#) of the WebUI.

Before installation, a network design should be planned and documented. A detailed network diagram prior to configuration and installation can help avoid costly, time-consuming adjustments after installation. Required information for installation and configuration of the D423 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 or CN).
- The MAC address for this radio's point-to-point partner radio.
- The MAC address for a **DN responder** — used to form a wireless link with another D423.
 - If [DN link auto-configuration](#) is being used, only the MAC address of the remote DN responder is needed. Other information is configured automatically.
 - If the [devices are being configured prior to installation](#), the MAC addresses for both DN responders in a DN to DN link are required. Additionally:
 - The polarity for both devices is required. Linked DNs must have opposite polarity (one even, the other odd).
 - The channel, Golay index and polarity.
- 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 D423 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.
- If VLAN will be used, 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.



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

- **Boresight:** Position the D423 at an azimuth that makes DN links as close to boresight as possible.
 - Because AltoPlex devices use a wide-angle beam pattern that can scan across a 90° horizontal and +/-20° vertical air space, boresight is not required but will create the strongest link.
- **Distance:** The shorter a link, the better the performance.

Powering the D423

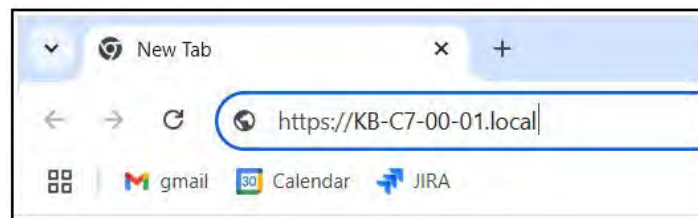
Power the D423 with a CE certified, standard IEEE Type 4 802.3bt Class 8 90W PoE injector or PoE switch.

Connecting to the D423

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. 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.

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

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).

Access the radio by using the management Wi-Fi access point

AltoPlex radios also provide a mechanism to access all radios through a management Wi-Fi access point, which is enabled by default but can be disabled. See [Wi-Fi connection to a D423](#) for more information.

Installation

Installation tips:

- Install the D423 on the pole or wall with no obstructions above the unit to allow for GPS synchronization.
- Maintain **clear line of sight (LOS)** at the front of the D423 so that links to other radios can be formed. Best performance is achieved with boresight alignment between D423 wireless devices, so this is recommended for DN to DN links. Because AltoPlex devices use a wide-angle beam pattern that can scan across a 90° horizontal and +/-20° vertical air space, boresight is not required but will create the strongest link.
- **Power source:** Power the D423 with a CE certified, standard IEEE Type 4 802.3bt Class 8 90W PoE injector or PoE switch.

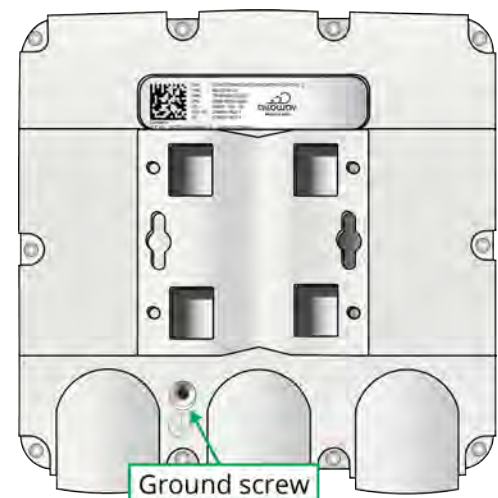
If a customer-supplied switch is used: To take advantage of the [LL discovery feature](#), the switch should support LLDP and it should be enabled. Also be aware that managed switches with Rapid Spanning Tree Protocol (RSTP) enabled increase the hop count for RSTP. See [Network tab — Spanning Tree Protocol configuration](#) for details about configuring AltoPlex devices for RSTP.

- When adjustments to positioning or aiming the D423 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.

Installation procedure

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

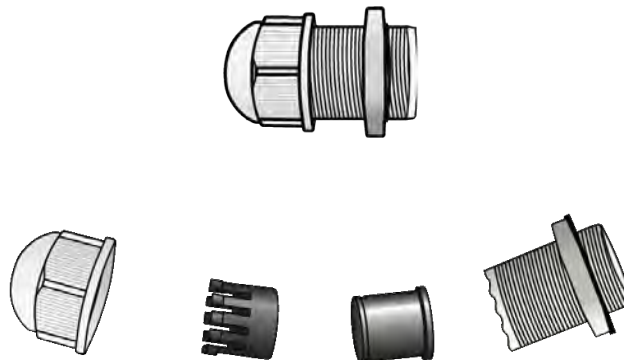
1. Install the ground wire, if required by code, at the installation location. Connect the other end of the ground wire to nearby good earth. The ground screw on AltoPlex devices is a #6-32 5/16th inch Phillips head screw.



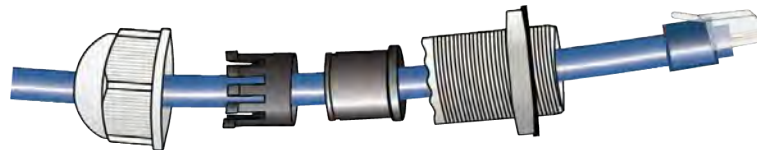
2. Install an outdoor-rated Ethernet cable through the provided cable gland and into port 1 on the D423 device:



- A. Unscrew and deconstruct the components of the gland.



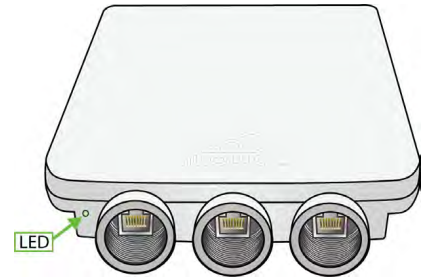
- B. Insert an outdoor-rated Cat5e (minimum) cable in the gland as shown.



- 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.
3. Repeat the above steps as necessary for ports 2 and 3.
4. 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 D423 according to the planned azimuth and elevation.
5. 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.



6. Verify that the device powers up. (LED is red during boot-up and then flashing green.)
7. If other D423s will be installed at the same site (for example, on the same pole), install them 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 D423 that will link to the first D423.
 - 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 [configured prior to mounting the devices](#).

9. For multi-link [daisy-chain](#) or [ring](#) topologies, install the remaining D423 devices according to the detailed network plan.
 - A. If [DN link auto-configuration](#) is being used in the field, configure each DN link in the field as the devices are installed.

Note: If the D423 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.

- B. Verify that each D423 is connected to the correct DN . This sample of the **Wireless** table on the [Status tab](#) shows the D423 connected to another DN (KB-C0-00-01).

Wireless												
Radio	MAC Address	Description	Chan	DN/ CN	Peer- Name	Link State	SNR	RSSI	TX MCS	TX Power Index	TX angles	RX angles
0	70:88:6b:c7:00:01	Techpubs radio 0	1	DN	KB-C7-00-01	UP 20:34:53	18/15	-56/-59	9/9	6/6	7/0 ~3.5/7.5	8.75/0 ~3.5/7.5

- C. **Check signal quality.** For example, a D423-D423 link should have an RSSI of greater than -65. Expected MCS for a D423-D423 link is 9 for up to 250 m, and 12 for up to 150 m with significant traffic.
10. After all DNs have been installed and linked, install client nodes one at a time, linking each to the appropriate DN. See [Configure links to client nodes](#) for information about linking CNs.

Configuration

The section contains the following information:

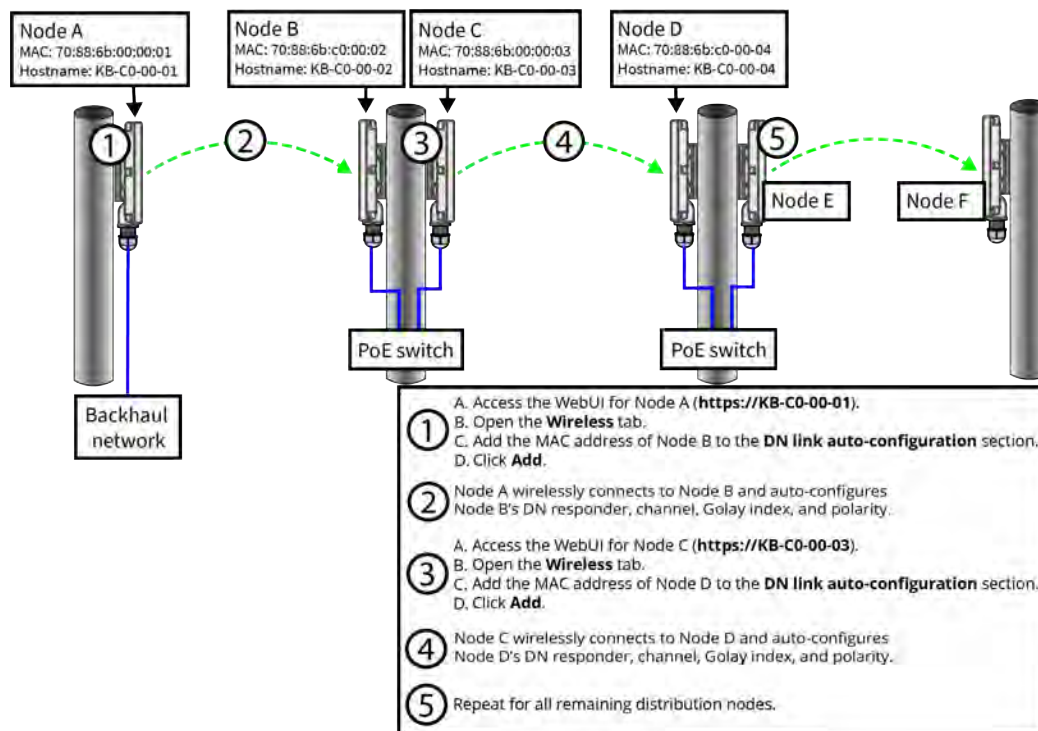
- [DN link auto-configuration](#)
- [Configure the connection to an AltoCommand server](#)
- [Configure links to client nodes](#)
- [Configuration via the WebUI](#)

DN link auto-configuration

Once that distribution nodes are installed, 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

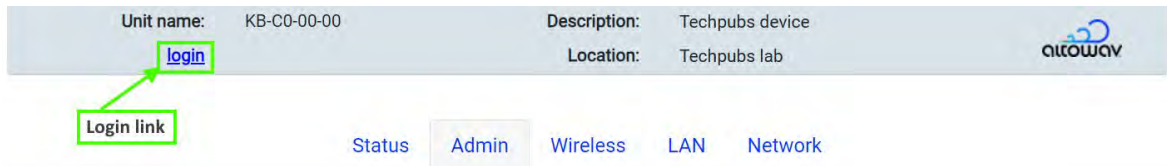
To auto-configure DN links:

1. Access the WebUI of the D423. 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 D423](#) for more information.

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



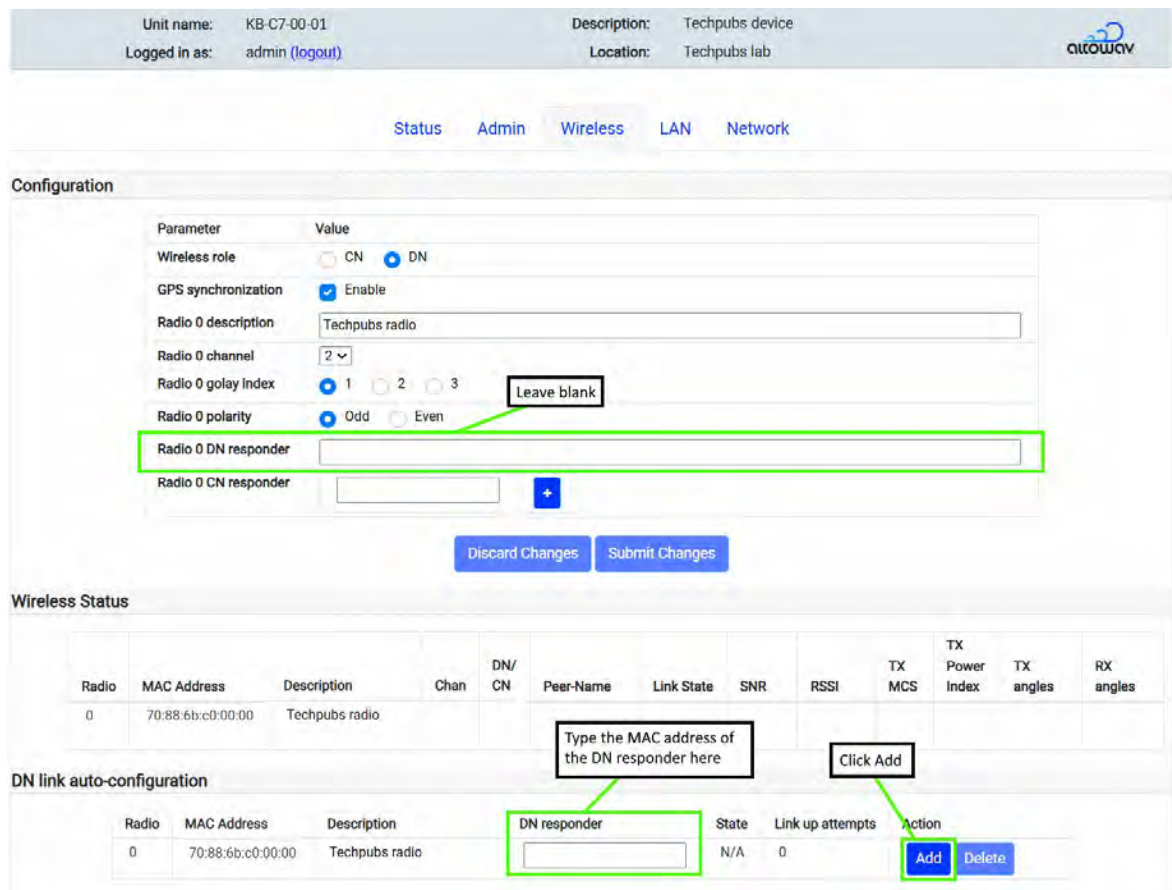
Unit name: KB-C0-00-00 Description: Techpubs device
Location: Techpubs lab

[login](#)

Login link

Status Admin Wireless LAN Network

- B. On the **Wireless** tab, in the **Configuration** section, leave the **Radio 0 DN responder** field blank.
- C. In the **DN link auto-configuration** section, type the MAC address of the **DN responder**.
- D. Click **Add**.



Unit name: KB-C7-00-01 Description: Techpubs device
Logged in as: admin (logout) Location: Techpubs lab

Status Admin Wireless LAN Network

Configuration

Parameter	Value
Wireless role	☐ CN ☒ DN
GPS synchronization	☒ Enable
Radio 0 description	Techpubs radio
Radio 0 channel	2
Radio 0 golay Index	☒ 1 ☐ 2 ☐ 3
Radio 0 polarity	☒ Odd ☐ Even
Radio 0 DN responder	
Radio 0 CN responder	

Discard Changes Submit Changes

Wireless Status

Radio	MAC Address	Description	Chan	DN/ CN	Peer-Name	Link State	SNR	RSSI	TX MCS	TX Power Index	TX angles	RX angles
0	70:88:6b:c0:00:00	Techpubs radio										

DN link auto-configuration

Radio	MAC Address	Description	DN responder	State	Link up attempts	Action
0	70:88:6b:c0:00:00	Techpubs radio		N/A	0	Add Delete

- 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. Access the WebUI for the DN responder (Node B in the above diagram).

Once the link between the initiator and the responder has been established, a link to the DN responder will appear in the **Peer-Name** column of the **Wireless Status** table.

Unit name: KB-C7-00-00

Logged in as: admin (logout)

Description: Techpubs device

Location: Techpubs lab



Status
Admin
Wireless
LAN
Network

Configuration

Parameter	Value
Wireless role	☐ CN ☒ DN
GPS synchronization	☒ Enable
Radio 0 description	Techpubs radio
Radio 0 channel	2
Radio 0 golay index	☒ 1 ☐ 2 ☐ 3
Radio 0 polarity	☒ Odd ☐ Even
Radio 0 DN responder	70:88:6b:c7:00:01
Radio 0 CN responder	+

Discard Changes
Submit Changes

Wireless Status

Radio	MAC Address	Description	Chan	DN/ CN	Peer-Name	State	Link Uptime	SNR	RSSI	TX MCS	Power Index	TX angles	RX angles
0	70:88:6b:c7:00:00	Techpubs radio	3	DN	KB-C7-00-01	UP	0 days 00:01:42	11/11	-62/-62	9/9	27/27	40/0 0/0	32/0 -8/0

DN link auto-configuration

Radio	MAC address	Description	DN responder	State	Link up attempts	Action
0	70:88:6b:c7:00:00	Techpubs radio		N/A	0	Add Delete

Click the link to open the DN responder's WebUI. The **Status** page is displayed.

If the switch connecting Node B and Node C is an unmanaged switch, or if it is a managed switch that is configured to forward LLDP data units, the hostname of Node C will be listed in the **LL Discovery** field.

Unit name: KB-C7-00-00
[login](#)

Description: Techpubs device
Location: Techpubs lab



Status
Admin
Wireless
LAN
Network

Device information

Techpubs

Device model: D423

Device role: DN

Ethernet MAC address: 70:88:6B:C7:00:00

Firmware version: 4.0.0

Device uptime: 4 days 15 hours 37 mins 03 secs

AltoCommand connection: Connected

GPS data:

Latitude	44.8608139	degrees
Longitude	-93.3608598	degrees
Altitude	283.846	meters

Device Temperature: No temperature sensor on this unit

Wireless

Radio	MAC Address	Description	Chan	DN/ CN	Peer- Name	Link State	SNR	RSSI	TX MCS	TX Power Index	TX angles	RX angles
0	70:88:6b:c7:00:01	Techpubs radio 0	1	CN	KB-C7-00-00	UP 20:34:53	18/15	-56/-59	9/9	6/6	7/0 -3.5/7.5	8.75/0 -3.5/7.5

LAN interfaces

Interface number	1	2	3
Enabled:	Yes	Yes	No
Status:	Connected	Connected	Not connected
Duplex:	Full	Full	N/A
Speed:	1000	1000	N/A
Maximum supported speed:	1 Gb/s	1 Gb/s	1 Gb/s
Power over ethernet:	Input	Output (PoE++) Enabled	Output (PoE++) Enabled
LL discovery:	KB-C7-00-02	None	None

Management interface

IP address:

10.0.0.2(dynamic)

Subnet mask:

255.255.255.0

Default gateway:

10.0.0.1

4. Access the WebUI for the next DN initiator (Node C in the above diagram).

- A. Click the link in the **LL Discovery** field of Node B's WebUI. This will open the WebUI for Node C.

If there is no link in the LL Discovery field, your switch may not be properly forwarding LLDP data units. In this case, access Node C's WebUI by using its hostname or IP address (**<https://<hostname>/>**).

- B. Click the **Wireless** tab.
- C. In the **Configuration** section, leave the **DN responder** field blank.
- D. In the **DN link auto-configuration** section, type the MAC address of the **DN responder**.
- E. Click **Add**.
- F. Perform other configuration as desired. See [Configuration via the WebUI](#).

5. Once the airlink is established, the DN responder will be auto-configured as described in step 2.
6. Continue this process for all of the distribution nodes in your system.

After the link between both distribution nodes has been established, perform [additional configuration](#) as necessary.

Delete the DN responder from the DN link auto-configuration

To delete the DN responder from the DN link auto-configuration, click **Delete**.

You can only delete a DN responder from the DN link auto-configuration prior to the DN responder responding to the incoming link request from the DN initiator. Once the link has been established, the **Delete** button will have no effect.

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. You can also configure the device after installation by using its [management Wi-Fi](#).

Testing links during bench configuration

By default, GPS is required to initiate links between devices. If you are testing radio links indoors, or in locations with weak GPS signals, the link may not properly form.

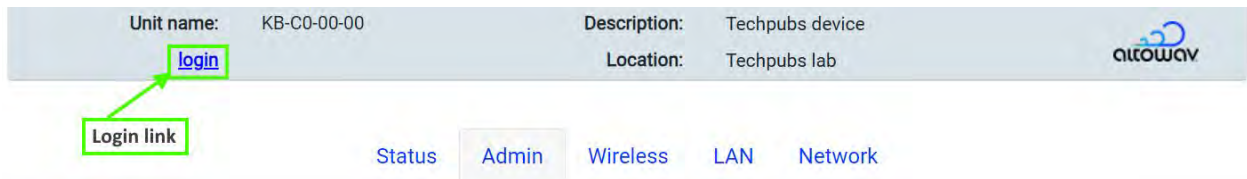
To test links, disable **GPS synchronization**. It is enabled by default.

1. Access the WebUI of the D423. In your browser's address bar, type:

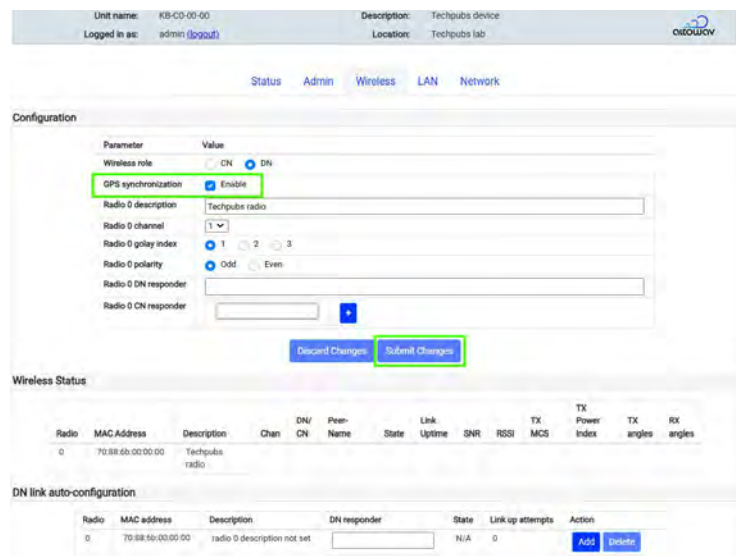
<https://hostname>

where *hostname* is the hostname (KB-XX-XX-XX) or IP address of the radio. See [Connecting to the D423](#) 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 **Wireless** tab.
4. Uncheck **GPS synchronization** to disable.
5. Click **Submit Changes**.



Note: Be sure to reenable GPS prior to installation in the field.

To check GPS status, click the **Status** tab:

Unit name: KB-C7-00-00
[login](#)

Description: Techpubs device
Location: Techpubs lab



Status Admin Wireless LAN Network

Device information

Device model: D423
Device role: DN
Ethernet MAC address: 70:88:6B:C7:00:00
Firmware version: 4.2.0
Device uptime: 4 days 15 hours 37 mins 03 secs
AltoCommand connection: Connected

GPS data: **Unsynchronized**

Device Temperature: No temperature sensor on this unit

Wireless

Waiting for GPS synchronization

Radio	MAC Address	Description	Chan	DN/ CN	Peer- Name	Link State	SNR	RSSI	TX MCS	TX Power Index	TX angles	RX angles
0	70:88:6b:c7:08:08	Techpubs radio										

LAN interfaces

Interface number	1	2	3
Enabled:	Yes	Yes	No
Status:	Connected	Connected	Not connected
Duplex:	Full	Full	N/A
Speed:	1000	1000	N/A
Maximum supported speed:	1 Gb/s	1 Gb/s	1 Gb/s
Power over ethernet:	Input	Output (PoE++) Enabled	Output (PoE++) Enabled
LL discovery:	KB-C7-00-01	None	None

Management interface

IP address: 10.0.0.2 (dynamic)
Subnet mask: 255.255.255.0
Default gateway: 10.0.0.1

Important: When using bench configuration, the following parameters must be configured on **both** distribution nodes or the link between them will not be successful:

- **Wireless tab, Configuration** section:
 - **Wireless role** — Must be set to the default of **DN**.
 - **Radio 0 DN responder** — Must be set to the MAC address of the other distribution node in the link.
 - **Channel** — Both distribution nodes must be set to the same channel.
 - **Golay index** — Both distribution nodes must be set to the same Golay index.
 - **Polarity** — Must be set to the opposite polarity of the other distribution node.

You can also perform [additional configuration](#) as necessary during bench configuration.

Configure a connection to an AltoCommand server

Beginning with release 3.9.1, AltoPlex distribution nodes can be configured to connect to an AltoCommand server. The AltoCommand server may be cloud-based, or may reside on the local network. Client nodes inherit the AltoCommand server from their linked distribution node. This feature requires AltoCommand version 4.0.

After the connection to the AltoCommand server has been configured on the AltoPlex radio, the radio sends an approval request to the server. A user on the AltoCommand server must approve the request, which will open a reverse tunnel for communication between the server and the radio.

To configure the connection to an AltoCommand server:

1. Access the WebUI of the D423. In your browser's address bar, type:

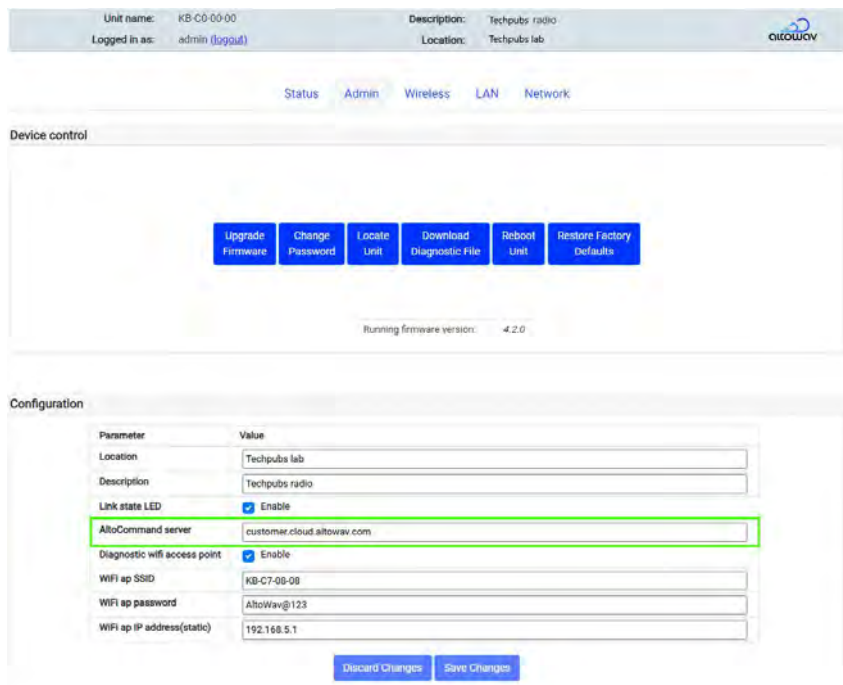
<https://hostname>

where *hostname* is the hostname (KB-XX-XX-XX) or IP address of the radio. See [Connecting to the D423](#) 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. In the **Configuration** section, for **AltoCommand server**, type the fully-qualified domain name or IP address of the AltoCommand server.
5. Click **Save Changes**.



View the status of the connection to the AltoCommand server

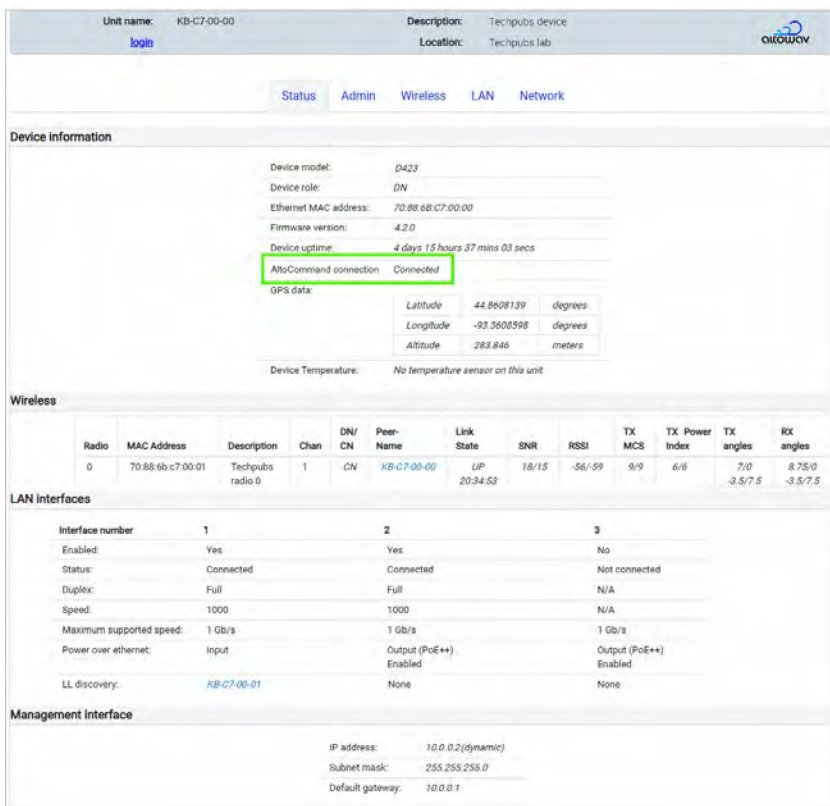
To view the status of the connection to the AltoCommand server:

1. Access the WebUI of the D423. 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 D423](#) for more information.

2. The **Device Information** section of the **Status** tab displays the current status of the **AltoCommand connection**.



The screenshot shows the WebUI of a D423 device. The top bar includes 'Unit name: KB-C7-00-00', 'Description: Techpubs device', and 'Location: Techpubs lab'. The 'Status' tab is selected, showing 'Device Information' with fields for Device model (D423), Device role (DN), Ethernet MAC address (70:88:68:C7:00:00), Firmware version (4.2.0), Device uptime (4 days 15 hours 37 mins 03 secs), and AltoCommand connection (Connected). Below this is a table for GPS data (Latitude, Longitude, Altitude) and a note about the temperature sensor. The 'Wireless' section shows a table with columns for Radio, MAC Address, Description, Chan, DN/CN, Peer-Name, Link State, SNR, RSSI, TX MCS, TX Power Index, TX angles, and RX angles. The 'LAN Interfaces' section shows a table with columns for Interface number, Enabled, Status, Duplex, Speed, Maximum supported speed, Power over ethernet, and LL discovery. The 'Management Interface' section shows fields for IP address, Subnet mask, and Default gateway.

Displayed values are:

- **Not configured** — The AltoCommand server has not been configured on the radio.
- **Disconnected** — The AltoCommand server has been configured on the radio but is not connected. Possible issues include an incorrect URL for the server, network access issues, etc.
- **Pending** — The AltoCommand server has been configured and successfully accessed, and the radio is waiting for the server to accept the connection.
- **Connected** — The radio is successfully connected to the configured AltoCommand server.

Configure links to client nodes

Note: Best practice is that links to client nodes should be created at the time that the client node is installed, rather than configuring the links prior to the client node being installed.

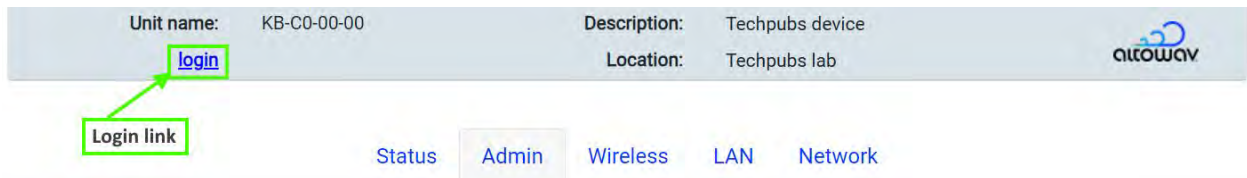
To add a link to a client node:

1. Access the WebUI of the D423. In your browser's address bar, type:

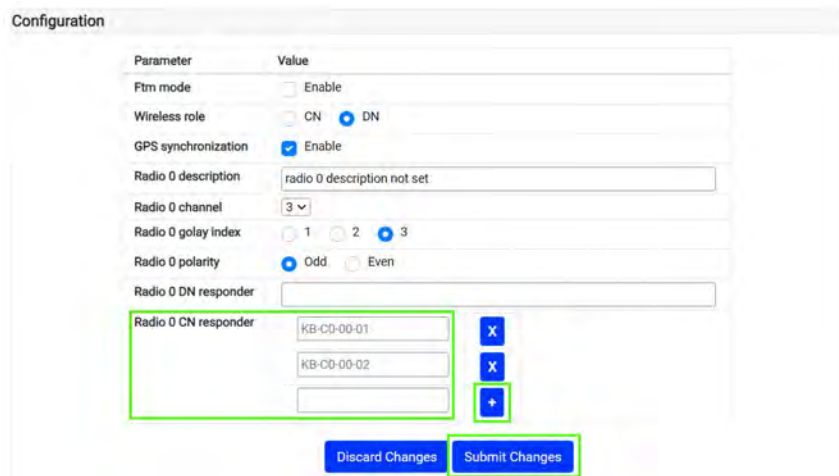
https://hostname

where *hostname* is the hostname (KB-XX-XX-XX) or IP address of the radio. See [Connecting to the D423](#) 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 **Wireless** tab.
4. In the **Configuration** section, for **CN responder**, type the hostname of the client node.
5. Click **+** to add additional client nodes.
 - To delete a client node, click **x**.
6. Click **Submit Changes**.

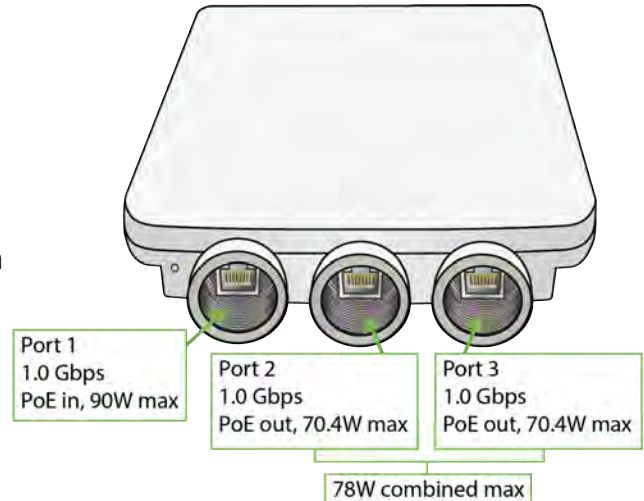


The airlink to the client node will be automatically established once its hostname has been added to the **CN responder** list.

Disable PoE output or data transmission for the Ethernet ports

The D423 has three Ethernet ports:

- Port 1 is enabled by default for data transmission.
 - Port 1 is also enabled for PoE input. PoE input cannot be disabled.
- Ports 2 and 3 are enabled by default for data transmission and PoE output.
 - 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.



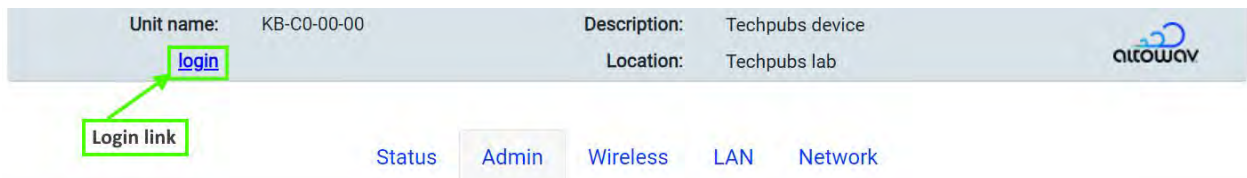
To disable either data transmission or PoE output:

1. Access the WebUI of the D423. 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 D423](#) for more information.

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



- Click the **LAN** tab.

The Interface table lists interfaces by number:

Interface number:	1	2	3
Port enable	☒ Enable	☒ Enable	☒ Enable
PoE enable	N/A	☒ Enable	☒ Enable

- To disable data transmission, for **Port enable**, click to toggle off **Enable**.
- To disable PoE output on port 2 and/or 3, for **PoE enable**, click to toggle off **Enable**.
- Click **Submit Changes**.

Configuration via the WebUI

The D423 can be configured through the WebUI. Access the WebUI by using one of the following methods:

- 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 D423](#) for more information.

- 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.

MAC Address	State	Channel	Remote MAC	Peer-Name	SNR Local/Remote	RSSI Local/Remote	TX MCS Local/Remote	TX Power Index Local/Remote
70:88:6b:c0:00:03	UP	4	70:88:6b:c0:00:04	KB-C0-00-04	11/12	-63/-62	9/9	12/7

- Use the device's [management Wi-Fi](#).
- 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, such as the firmware version data-keyref="management-UI">AltoCommand server status, and wireless connections, on the [Status tab](#). You can also click on a **Peer-Name** to access the WebUI for a connected device.
- On the [Admin tab](#):
 - Configure the location of your AltoCommand server. (Requires AltoCommand version 4.0).
 - [Upgrade firmware](#).
 - [Change the admin password](#).
 - Locate the radio.
 - [Download a diagnostic file](#).
 - [Reboot](#).
 - [Restore Factory Defaults](#).
 - Set the **Location** or **Description** per your network design plan.
 - [Configure diagnostic Wi-Fi settings](#).
- On the [Wireless tab](#):
 - Configure the role of the radio, either distribution node (**DN**) or client node (**CN**).
 - If the radio is configured to use the DN role:

- Configure the radio's **Channel**, **Golay index**, and **Polarity**, as well as optionally configure a link to another DN, or use [DN link auto-configuration](#).
- [Configure CN links](#) for up to 15 client nodes.
- On the [LAN tab](#), configure [MAC filtering](#).
- On the [Network tab](#), configuration various networking features, such as VLANs, Spanning Tree protocol, and the management interface.

The header of the WebUI shows the **Unit name** of the D423 (also called the hostname), **Description** and **Location**, as well as offering a **login** link.

Unit name: KB-C0-00-00 login	Description: Techpubs device Location: Techpubs lab	
Status Admin Wireless LAN Network		

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

Unit name: KB-C0-00-00 login	Description: Techpubs device Location: Techpubs lab	
Status Admin Wireless LAN Network		

Status tab

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

Unit name: KB-C7-00-00 login	Description: Techpubs device Location: Techpubs lab												
Status Admin Wireless LAN Network													
Device Information													
Device model: D423 Device role: DN Ethernet MAC address: 70:88:6B:C7:00:00 Firmware version: 4.2.0 Device uptime: 4 days 15 hours 37 mins 00 secs Airtoway connection: Connected GPS data: Latitude: 44.8608139 degrees Longitude: -83.2600980 degrees Altitude: 283.840 meters Device Temperature: No temperature sensor on this unit													
Wireless													
Radio	MAC Address	Description	Chan	DN	Peer Name	Link State	SNR	RSSI	TX MCS	TX Index	TX Power	TX angles	RX angles
0	70:88:6B:C7:00:01	Techpubs radio 0	1	CN	KB-C7-00-00	UP	20.24.53	18/15	-66/-29	0/0	6/6	7/0	-8.5/7.8
LAN Interfaces													
Interface number	1	2	3										
Enabled	Yes	Yes	No										
Status	Connected	Connected	Not connected										
Duplex	Full	Full	N/A										
Speed	1000	1000	N/A										
Maximum supported speed	1 Gb/s	1 Gb/s	1 Gb/s										
Power over ethernet	Input	Output (PoE+)	Output (PoE+)										
LL discovery	70:88:6B:C7:00:01	None	None										
Management Interface													
IP address: 10.0.0.2 (dynamic) Subnet mask: 255.255.255.0 Default gateway: 10.0.0.1													

Status tab — Device Information section

This section displays:

- The Device model name (D423).
- The Device role — distribution node (**DN**) or client node (**CN**).
- The MAC address.
- The current firmware version.

It is generally recommended that all devices in the network use the same firmware version. See [Upgrading Firmware](#) for information about upgrading the radio's firmware.

- Device uptime.
- AltoCommand server status. (This feature requires AltoCommand version 4.0.)

Displayed values are:

- **Not configured** — The AltoCommand server has not been configured on the radio.
- **Disconnected** — The AltoCommand server has been configured on the radio but is not connected. Possible issues include an incorrect URL for the server, network access issues, etc.
- **Pending** — The AltoCommand server has been configured and successfully accessed, and the radio is waiting for the server to accept the connection.
- **Connected** — The radio is successfully connected to the configured AltoCommand server.
- GPS data.
- Device temperature.

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.

Wireless													
Radio	MAC Address	Description	Chan	DN/ CN	Peer- Name	Link State	SNR	RSSI	TX MCS	TX Power Index	TX angles	RX angles	
0	70:88:6b:c7:00:01	Techpubs radio 0	1	DN	KB-C7-00-01	UP 20:34:53	18/15	-56/-59	9/9	6/6	7/0 -3.5/7.5	8.75/0 -3.5/7.5	

- **Link State** lists the state of the link and the length of time that the link has been up or down. Values are:
 - **Up** — The link is functioning normally.
 - **Up but blocked** — The link is formed but is being blocked by [Spanning Tree Protocol](#).
 - **Down** — The link is down. Includes the number of unsuccessful linkup attempts.

- **SNR, RSSI, TX MCS, TX Power Index, TX angles**, and **RX angles** show values for both ends of the link, in local/remote order.
- **TX angles** and **RX angles** refer to the beam angle when looking from behind the radio towards the linked peer.
 - A positive value refers to the beam angle to the right of boresight.
 - A negative value refers to the beam angle to the left of boresight.

Tip: The hostnames listed under **Peer-Name** are clickable links and will open the radio's WebUI in a new browser tab.

Status tab — LAN interfaces section

This section shows information for the LAN interface (Port 1 for the D423), 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**, **Subnet mask** and **Default gateway** of the radio's management interface. The IP address field also displays whether the radio is configured to have a dynamic IP address assigned by an upstream DHCP server, or a static IP address. See [Management Network Interface Configuration](#) for more information.

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.

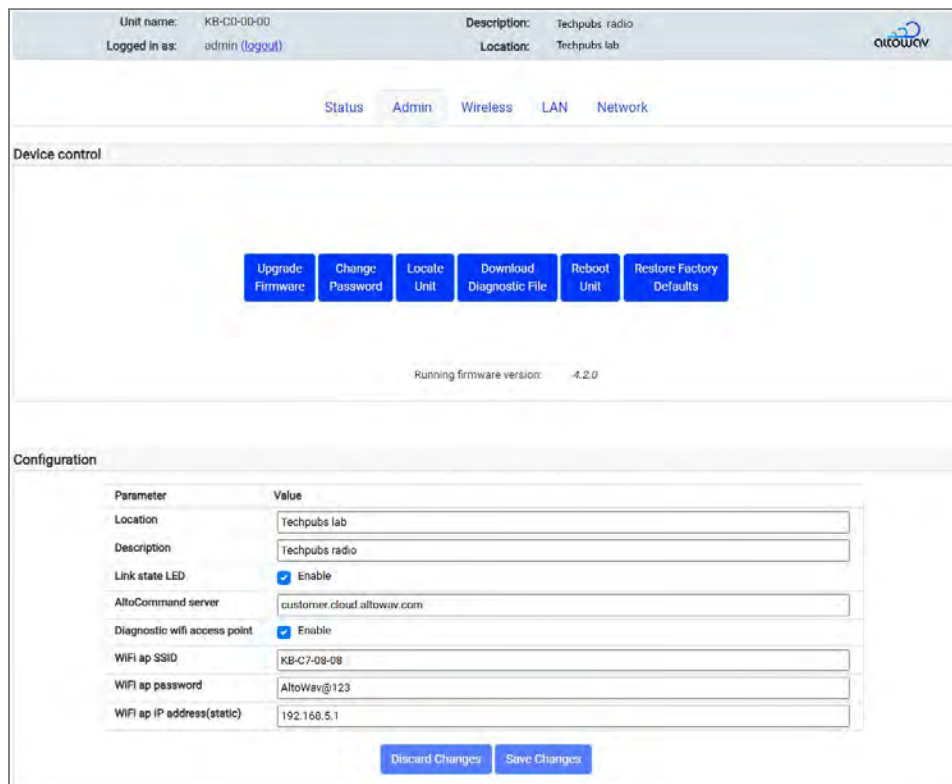
Click the **login** link in the WebUI header to log in as administrator. The default password is **admin**.



Unit name:	KB-C0-00-00	Description:	Techpubs device
	login	Location:	Techpubs lab

[Status](#)
[Admin](#)
[Wireless](#)
[LAN](#)
[Network](#)

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



Unit name:	KB-C0-00-00	Description:	Techpubs radio
Logged in as:	admin (logout)	Location:	Techpubs lab

[Status](#)
[Admin](#)
[Wireless](#)
[LAN](#)
[Network](#)

Device control

[Upgrade Firmware](#)
[Change Password](#)
[Locate Unit](#)
[Download Diagnostic File](#)
[Reboot Unit](#)
[Restore Factory Defaults](#)

Running firmware version: 4.2.0

Configuration

Parameter	Value
Location	Techpubs lab
Description	Techpubs radio
Link state LED	☒ Enable
AltoCommand server	customer.cloud.altowav.com
D diagnostic wifi access point	☒ Enable
WiFi ap SSID	KB-C7-08-08
WiFi ap password	AltoWav@123
WiFi ap IP address(static)	192.168.5.1

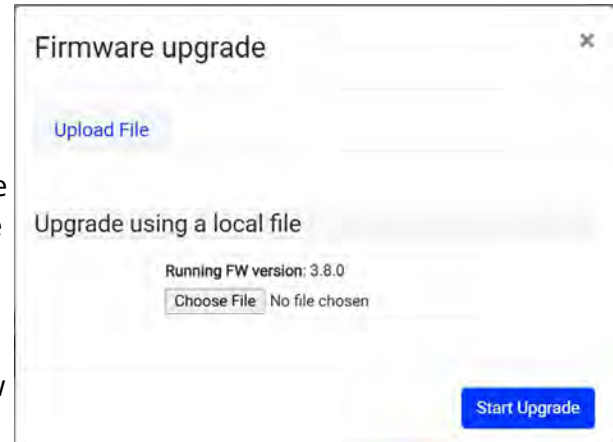
[Discard Changes](#)
[Save Changes](#)

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](#).

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. See the [AltoCommand User Guide](#) for more information.



Change Password — Use this button to change the password for the admin of the D423. 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](#).

AltoCommand server — Configures the radio to connect to the specified AltoCommand server. See [Configure the connection to an AltoCommand server](#) for more information.

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

The Wireless tab includes configuration of the device's wireless role, a GPS synchronization checkbox, radio description, channel, Golay index, polarity, DN responder, and list of CN responders. You can also change the 60 GHz airlink SSID and password from the Wireless tab. 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.

Unit name: KB-C7-00-00
Logged in as: admin (logout)

Description: Techpubs device
Location: Techpubs lab



[Status](#)
[Admin](#)
[Wireless](#)
[LAN](#)
[Network](#)

Configuration

Parameter	Value
Wireless role	☐ CN ☒ DN
GPS synchronization	☐ Enable
Radio 0 description	Techpubs radio
Radio 0 channel	2
Radio 0 golay index	☒ 1 ☐ 2 ☐ 3
Radio 0 polarity	☒ Odd ☐ Even
Radio 0 DN responder	
Radio 0 CN responder	KB-C7-08-3E X +

Discard Changes
Submit Changes

Wireless Status

Radio	MAC Address	Description	Chan	DN/ CN	Peer-Name	Link State	SNR	RSSI	Tx MCS	Tx Power Index	Tx angles	Rx angles
0	70:88:6b:c7:00:00	Techpubs radio										

DN link auto-configuration

Radio	MAC address	Description	DN responder	State	Link up attempts	Action
0	70:88:6b:c7:00:00	Techpubs radio		N/A	0	Add Delete

Wireless Security

Parameter	Value
60 ghz airlink SSID	[default]
60 ghz airlink encryption passkey	[default-passkey]

Discard Changes
Submit Changes

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 — Selects whether the device will act as a DN (distribution node) or a CN (client node). Default setting is DN. A DN can form a wireless link to one other DN and up to 15 CNs. A CN can be linked wirelessly to only one DN. See **DN responder** and **CN responder** below.

GPS synchronization — Enables or disables GPS synchronization. The D423 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 [Design and deployment](#).

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. This field is only enabled when the Wireless Role of DN is selected for this device.

CN responder sets a list of hostnames (KB-XX-XX-XX) for up to 15 connected clients. It is best practice to add a CN responder to this list at the time of installation, not before.

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.

Wireless													
Radio	MAC Address	Description	Chan	DN/ CN	Peer- Name	Link State	SNR	RSSI	TX MCS	TX Power Index	TX angles	RX angles	
0	70:88:6b:c7:00:01	Techpubs radio 0	1	DN	KB-C7-00-01	UP 20:34:53	18/15	-56/-59	9/9	6/6	7/0 -3.5/7.5	8.75/0 -3.5/7.5	

- **Link State** lists the state of the link and the length of time that the link has been up or down. Values are:
 - **Up** — The link is functioning normally.
 - **Up but blocked** — The link is formed but is being blocked by [Spanning Tree Protocol](#).
 - **Down** — The link is down. Includes the number of unsuccessful linkup attempts.
- **SNR, RSSI, TX MCS, TX Power Index, TX angles, and RX angles** show values for both ends of the link, in local/remote order.
- **TX angles** and **RX angles** refer to the beam angle when looking from behind the radio towards the linked peer.
 - A positive value refers to the beam angle to the right of boresight.
 - A negative value refers to the beam angle to the left of boresight.

Tip: The hostnames listed under **Peer-Name** are clickable links and will open the radio's WebUI in a new browser tab.

Wireless tab — DN link auto-configuration section

See [DN link auto-configuration](#) for information about the **DN link auto-configuration** section.

Wireless tab — Wireless Security section

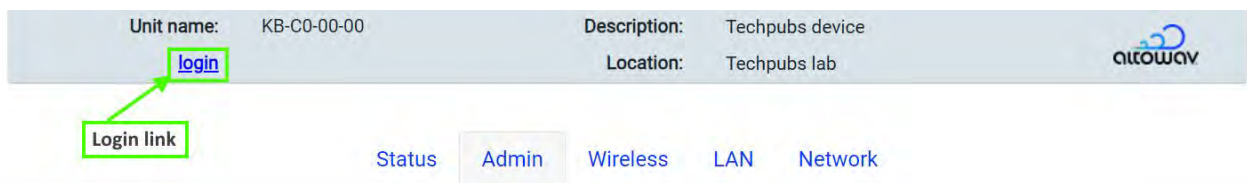
All AltoPlex devices have the same default SSID and encryption passkey for their 60 GHz airlink. Generally, this is sufficient because the devices will only form links to radios that are specified in their configuration.

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 D423.

Unit name: KB-C0-00-00

Description: Techpubs device



Logged in as: admin ([logout](#))

Location: Techpubs lab

Status
Admin
Wireless
LAN
Network

Ethernet Port Configuration

Interface number:	1	2	3
Port enable	☒ Enable	☒ Enable	☒ Enable
PoE enable	N/A	☐ Enable	☐ Enable

Discard Changes
Submit Changes



MAC Filter Configuration

Parameter	Value
Ethernet port 1 mac limit	Unlimited ▼
Ethernet port 1 destination mac address	
Ethernet port 1 unicast conversion	☐ Enable
Ethernet port 2 mac limit	Unlimited ▼
Ethernet port 2 destination mac address	
Ethernet port 2 unicast conversion	☐ Enable
Ethernet port 3 mac limit	Unlimited ▼
Ethernet port 3 destination mac address	
Ethernet port 3 unicast conversion	☐ Enable

Discard Changes
Submit Changes

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.

Tip: 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 [Connecting to the D423](#) 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 top half of the **Network** tab contains Network Reachability Configuration settings. They include settings for Management Network Interfaces, VLAN Configuration and Port Isolation.

Unit name: KB-C0-01-14
Description: system description not set

Logged in as: admin ([logout](#))
Location: system location not set

Status
Admin
Wireless
LAN
Network

Network Reachability Configuration

Management Network Interface Configuration

Parameter	Value
IP assignment method	☐ Static ☒ Dynamic
IP address (static)	192.168.0.1
Network mask (static)	255.255.0.0
Network gateway (static)	192.168.0.1

Virtual LAN Configuration

Parameter	Value
VLAN 802.1q mode	☒ Disable ☐ Enable
Management 802.1q VLAN ID	1
Ethernet port 1 802.1q accepted frame types	☒ All ☐ Tagged
Ethernet port 1 802.1q PVID	1
Ethernet port 1 802.1q membership	1

Port Isolation

Parameter	Value
Ethernet port 1 isolation	☐ Enable
Wireless port isolation	☐ Enable

Discard Changes
Submit Changes

Network tab — Network Reachability Configuration section

Management Network Interface Configuration

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 factory default fallback IP.

- 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.
- For radios with a firmware release prior to 3.6.0, the factory default fallback IP address will be the address that was included on the sticker when the device was originally shipped.

Click **Static** to configure the radio to use a static IP address rather than dynamic IP address assignment. Configure the **IP address**, **Network mask** and **Network gateway**.

Virtual LAN Configuration

Note: With AltoPlex technology, a D423 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.

VLAN 802.1q mode — Select **Enable** to enable VLAN support on this radio.

Management 802.1q VLAN ID — The identification number of the VLAN used for management purposes.

Ethernet port x 802.1q accepted frame types — For VLANs that the port is a member of, accept **All** incoming Ethernet packets, or only packets that are **Tagged**.

Ethernet port x 802.1q PVID — The Port VLAN ID (PVID). This determines what VLAN ID will be assigned to untagged frames.

Ethernet port x 802.1q membership — The VLANs that this Ethernet Port is a member of. Allowed values are single integers, a range of integers, or both. Values should be comma-separated without spaces. For example, 1,6,10-15. Maximum value is 4094.

Ethernet port x isolation — Click **Enabled** to restrict traffic between nodes in the VLAN over the Ethernet interface.

Wireless port isolation — Click **Enabled** to restrict traffic between nodes in the VLAN over the Wireless interface.

Network tab — Spanning Tree Protocol Configuration

Spanning Tree Protocol Configuration

Parameter	Value
Spanning tree protocol (stp) enable	☐ Enable
STP bridge priority	8
STP radio 0 port path cost	20000
STP Ethernet port 1 bpdu filter	☐ Enable

Discard Changes
Submit Changes

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.

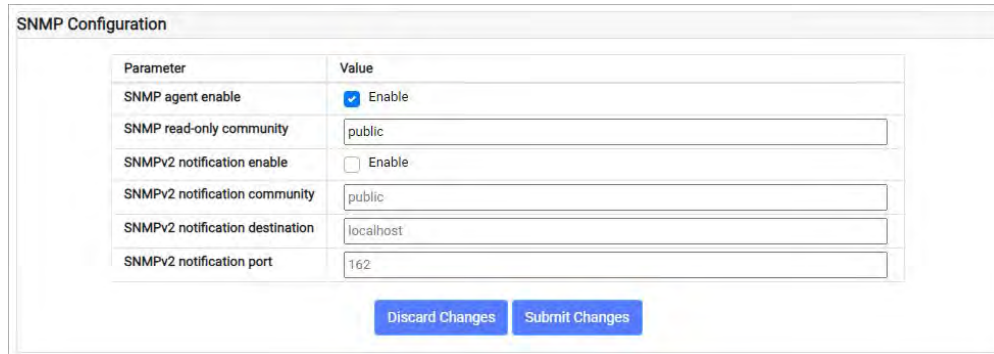
STP bridge priority is used to determine which device will serve as the root of the spanning tree. The device with the lowest priority will serve as the root. The priority configured here is a multiplier; to determine the actual STP priority, multiply by 4096.

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.



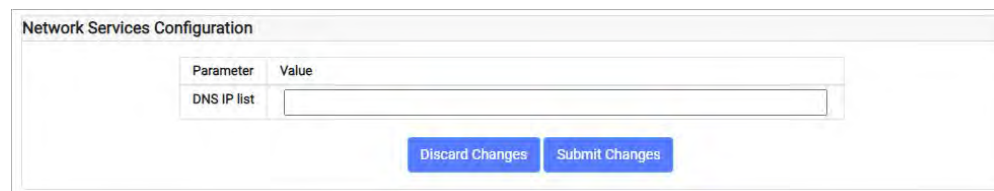
Parameter	Value
SNMP agent enable	☒ Enable
SNMP read-only community	public
SNMPv2 notification enable	☐ Enable
SNMPv2 notification community	public
SNMPv2 notification destination	localhost
SNMPv2 notification port	162

Discard Changes Submit Changes

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.



Parameter	Value
DNS IP list	

Discard Changes Submit Changes

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 D423's Ethernet port, in ASCII format), or the **Hostif** (the hostname:Ethernet_port of the D423 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 forwarded, with the circuit ID appended.

Note: All wireless links are automatically considered trusted.

DHCP Relay Configuration (Option 82)

Parameter	Value
DHCP relay agent enable	☐ Enable
DHCP relay agent circuit ID type	☒ Hwaddr ☐ Hostif
Ethernet port 1 host access	☒ Trusted ☐ Untrusted

Discard Changes
Submit Changes

Maintenance and security

Wi-Fi connection to a D423

Connect to a D423 via Wi-Fi to access the WebUI for diagnostic purposes and configuration tasks, if required.

Note: The Wi-Fi connection to the D423 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.

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

Parameter	Value
Location	Techpubs lab
Description	Techpubs device
Link state LED	☒ Enable
AltoCommand server	cloud.altocommand.altowav.com
Diagnostic wifi access point	☒ Enable
WiFi ap SSID	KB-C7-00-01
WiFi ap password	AltoWav@123
WiFi ap IP address(static)	192.168.5.1
Hide SSID	☐ Enable

[Discard Changes](#)
[Save Changes](#)

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 D423 via Wi-Fi:

- You must be in close range to the D423 in order to connect to it via Wi-Fi — generally within 10 - 20 ft.
- A D423 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.

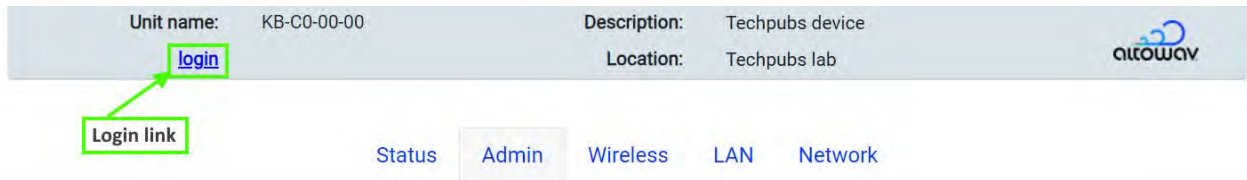
To change the device password:

1. Access the WebUI of the D423. 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 D423](#) 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 D423 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 D423.

Note: This procedure describes how to upload an SSH key to the D423. 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 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 [Connecting to the D423](#) 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](https://support.altowav.com) 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 and P621 devices.
 - **DEVO** — Firmware used for D423, 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](http://support.altoway.com) at support.altoway.com.

The following files are included in the firmware zip file:

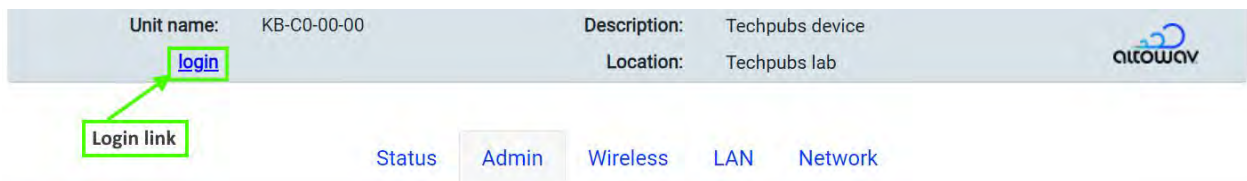
- A digest file, not used as part of this upgrade process.
- The firmware binary. See [The upgrade software filename](#) for information about the filename used for the firmware binary.

2. Access the WebUI of the D423. In your browser's address bar, type:

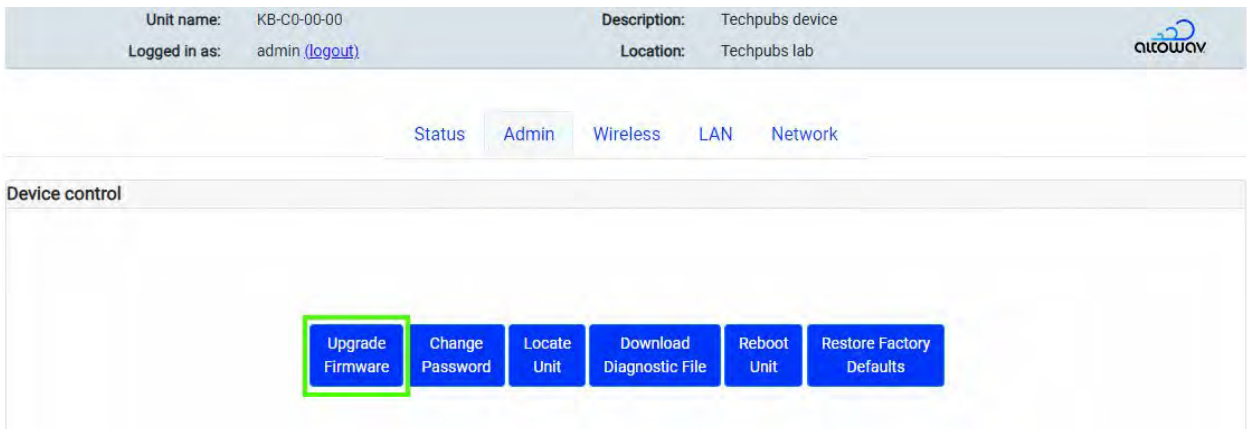
`https://hostname`

where *hostname* is the hostname (KB-XX-XX-XX) or IP address of the radio. See [Connecting to the D423](#) for more information.

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

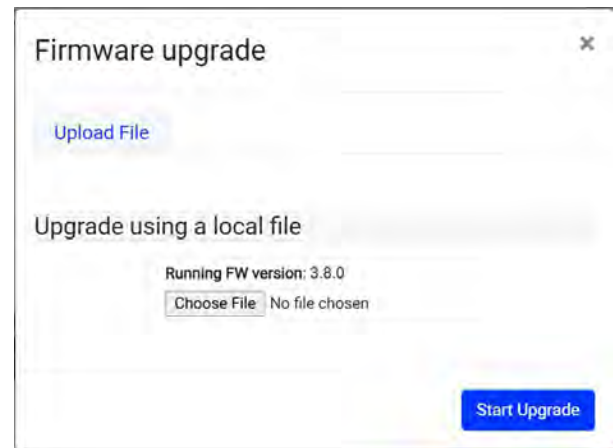


4. Click the **Admin** tab.
5. Click the **Upgrade Firmware** button.



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 D423 and install the file:

1. Download and unzip the firmware zip file from [Altoplex Firmware Downloads](http://support.altoway.com) at support.altoway.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 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 [Connecting to the D423](#) 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 D423. 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](http://support.altowav.com) 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 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 [Connecting to the D423](#) 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 D423. 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](https://support.altoway.com) at support.altoway.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
{
```

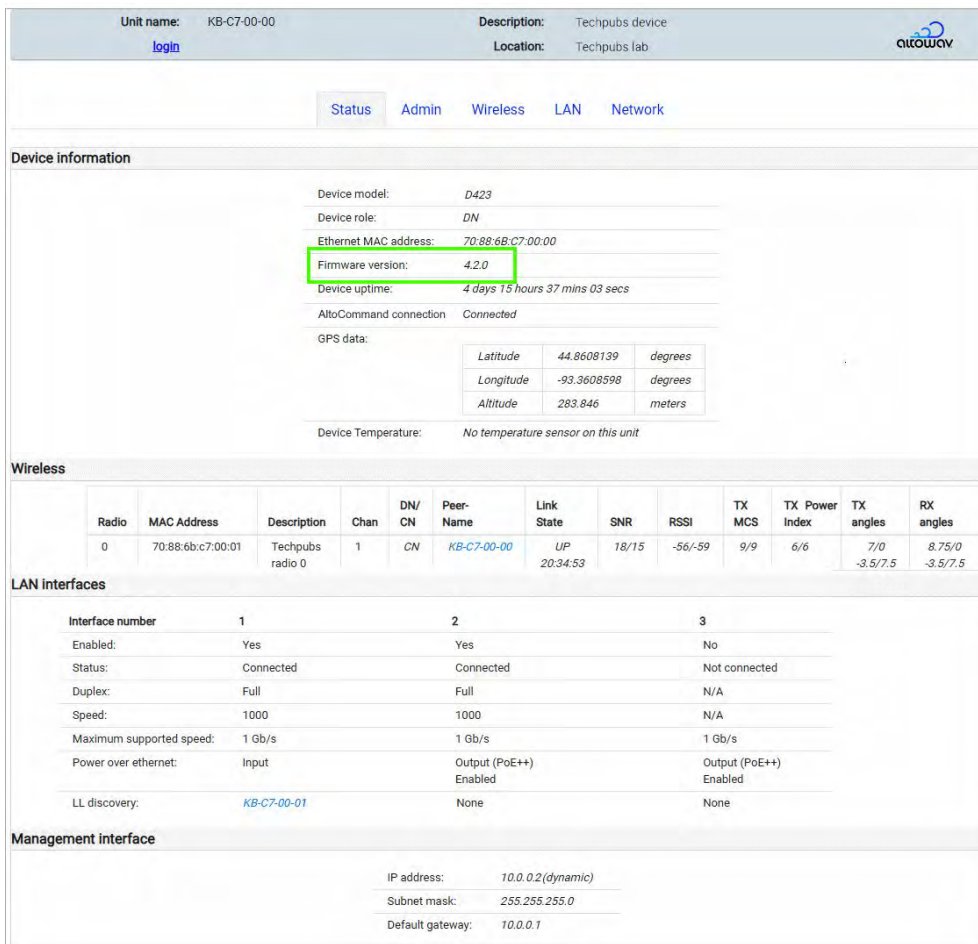
```
"status":"starting",
"running-sw-version":"3.9.1",
"upgrade-running":"yes"
}
```

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:



The screenshot shows the WebUI interface for a D423 device. The top bar displays the unit name 'KB-C7-00-00', description 'Techpubs device', location 'Techpubs lab', and a 'login' link. Below this are tabs for 'Status', 'Admin', 'Wireless', 'LAN', and 'Network'. The 'Status' tab is active, showing the 'Device information' section. In this section, the 'Firmware version' is highlighted with a green box and shows '4.2.0'. Other details include device model 'D423', device role 'DN', Ethernet MAC address '70:88:6B:C7:00:00', device uptime '4 days 15 hours 37 mins 03 secs', and AltoCommand connection 'Connected'. GPS data is also shown with latitude, longitude, and altitude. Below this is the 'Wireless' section with a table of radio details. The 'LAN interfaces' section shows three interfaces with their respective status and configuration. The 'Management interface' section shows the IP address, subnet mask, and default gateway.

Radio	MAC Address	Description	Chan	DN/ CN	Peer- Name	Link State	SNR	RSSI	TX MCS	TX Power Index	TX angles	RX angles
0	70:88:6b:c7:00:01	Techpubs radio 0	1	CN	KB-C7-00-00	UP	18/15	-56/-59	9/9	6/6	7/0 -3.5/7.5	8.75/0 -3.5/7.5

Interface number	1	2	3
Enabled:	Yes	Yes	No
Status:	Connected	Connected	Not connected
Duplex:	Full	Full	N/A
Speed:	1000	1000	N/A
Maximum supported speed:	1 Gb/s	1 Gb/s	1 Gb/s
Power over ethernet:	Input	Output (PoE++)	Output (PoE++)
		Enabled	Enabled
LL discovery:	KB-C7-00-01	None	None

Management interface
IP address: 10.0.0.2(dynamic)
Subnet mask: 255.255.255.0
Default gateway: 10.0.0.1

Verify firmware update from the command line

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 [Connecting to the D423](#) 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" : "DN",
  "Number Ethernet Interfaces" : 1,
  "Number RF Interfaces" : 1,
  "Part number" : "1900-8411-1012-devo-2-LBKA0ZZ1SV1",
  "Serial number" : "000000000000000000000001KB-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

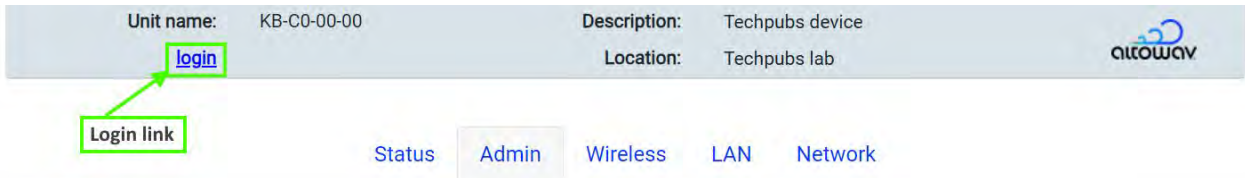
Note: A power-cycle or reboot clears the diagnostic log information stored in the device. So during troubleshooting, you should capture the diagnostic log in a file, before the power-cycle or reboot. If you require troubleshooting assistance, information in the diagnostic log may be useful.

1. Access the WebUI of the D423. 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 D423](#) 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.



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 reset the device.

1. Access the WebUI of the D423. 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 D423](#) 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.



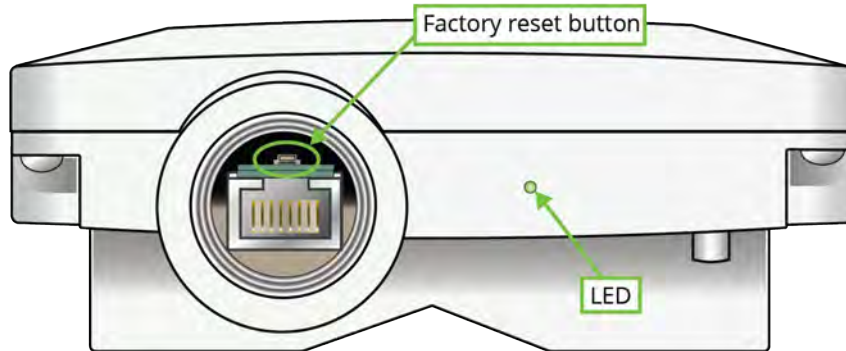
5. A confirmation dialog opens. Enter the text **confirm factory reset** and click **OK**.

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.

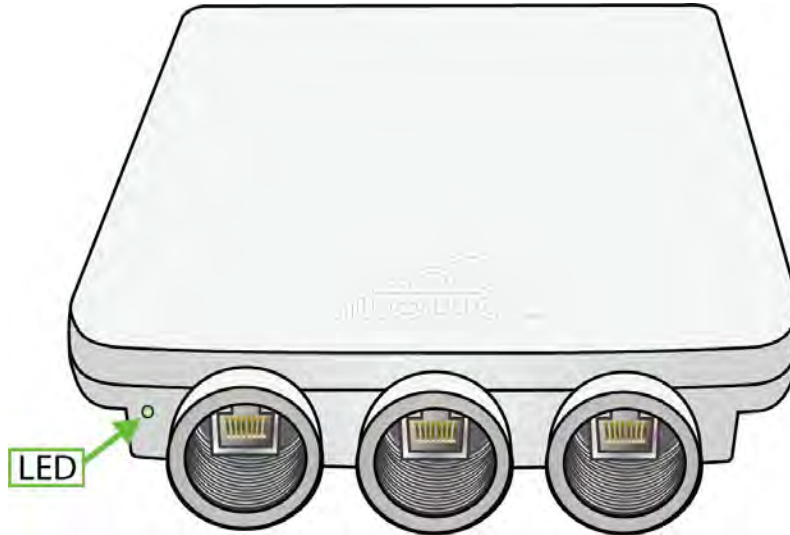
Troubleshooting

This chapter contains the following topics:

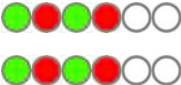
- [LED Indicators](#)
- [Lost Password](#)
- [Download a Diagnostic File](#)
- [MAC addresses used by the D423](#)

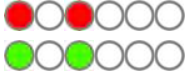
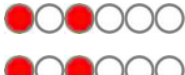
LED Indicators

The D423 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. Only applies if the device is functioning in a distribution node (DN) role. If the device is the wireless responder in a DN-DN link, 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 D423 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.

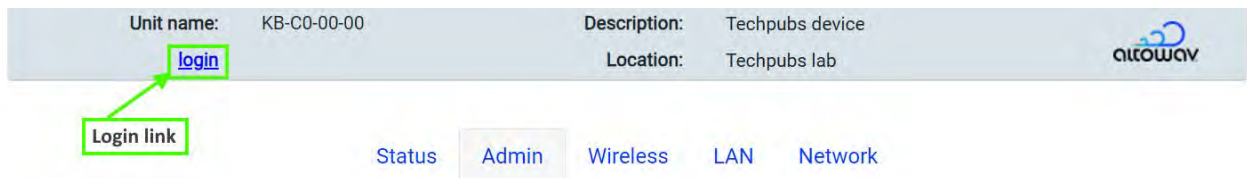
Follow these steps to download a diagnostic file for connected devices from the WebUI:

1. Access the WebUI of the D423. In your browser's address bar, type:

`https://hostname`

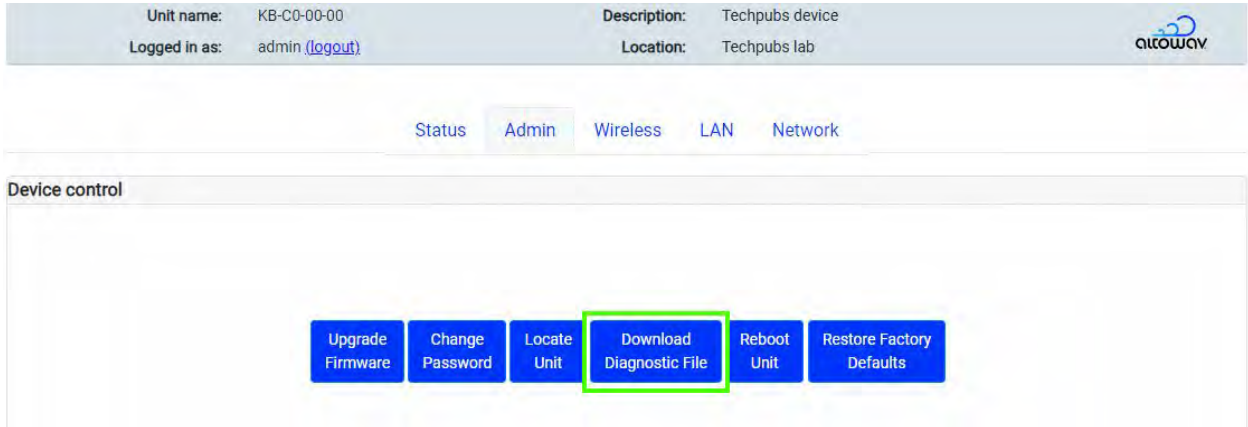
where *hostname* is the hostname (KB-XX-XX-XX) or IP address of the radio. See [Connecting to the D423](#) for more information.

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.

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



- 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
- 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

- 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.
- 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 D423

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 .

DN — See .

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 wireless 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 that initially establishes a link with a remote device. By default, the initiator 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.

