

Altoway AltoPlex Series C410 and C420 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 NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

Altowav would like to thank all of our staff for their efforts and expertise in development and implementation of the C410 and C420.

© 2024-2025 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 C410 and C420 device complies with FCC radiation exposure limits set forth for an uncontrolled environment. A minimum of 35 centimeters (14 inches) of separation between the C410 and C420 and all persons shall be maintained.

FCC Regulatory Statement

The C410 and C420 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 C410 and C420 device complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. A minimum of 35 centimeters of separation between the C410 and C420 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 C410 and C420 et toutes les personnes doit être maintenu.

ISED Industry Canada Regulatory Statement

The C410 and C420 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 C410 and C420:

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
<p>Updated for the 4.2.0 software release:</p> <ul style="list-style-type: none"> • 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
<p>Updated for the 3.9.1 software release:</p> <ul style="list-style-type: none"> • Added information about AltoCommand Cloud Connection. (Does not apply to the C410/C420 User Guide.) • Added regulatory information for ETSI certification. 	08/11/2025
<p>Updated for the 3.6.0 software release:</p> <ul style="list-style-type: none"> • Added MAC filtering. • Added information about the factory default fallback static IP address of 192.168.0.1, new to release 3.6.0. • Added link to the AltoWay enterprise MIB 	05/05/2025
<p>Updated for the 3.3.1 release:</p> <ul style="list-style-type: none"> • LL Discovery information added to the Status page . • Updated VLAN configuration information. • Upgrading Firmware procedures updated. 	02/05/2025
<p>Initial release of the C410 and C420.</p>	12/18/2024

Contents

C410 and C420 User Guide overview	7
Additional Documents.....	7
Additional help	7
Introduction	8
C410/C420 installation and configuration	9
Tool List.....	9
Box contents	9
Mounting brackets.....	10
About the C410 and C420	12
Requirements for deployment.....	12
Installation steps	13
Connecting to the C410 and C420	16
C410/C420 Configuration via WebUI.....	19
Maintenance and security	30
Change the device password.....	30
Enable Passwordless SSH	31
Upgrading firmware.....	32
Reboot a device	39
Factory reset	40
Troubleshooting	42
LED Indicators.....	43
Lost Password.....	44
Download a Diagnostic File.....	44
MAC addresses used by the C410 and C420.....	46
Glossary	47

C410 and C420 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 C410 and C420 devices.

This guide is intended for network and system administrators who will install, configure, and manage Altowav networks using C410 and C420 devices.

This guide includes instructions for the installation, configuration and management of C410 and C420 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 C410 and C420 devices:

- For general technology specifications and product datasheets, see altowav.com/technology/
- [C410 and C420 Quick Start Guide](#)
- [D621 User Guide](#)
- [Altowav AltoCommand User Guide](#)

Additional help

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

Web	support.altowav.com
-----	--

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

Introduction

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

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

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

- Gigabit fixed-wireless access (FWA).
- Surveillance camera connectivity.
- Multi-dwelling unit distribution.

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

C410/C420 installation and configuration

The installation instructions for C410 and C420 radios include:

- Tool list.
- C410/C420 box contents.
- Mounting instructions.
- Functional description.
- A list of the network design information required.
- Installation and configuration steps.
- Configuration example.

Tool List

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

Box contents

- C410/C420 device.
- IP67 cable gland.
- Indoor Power over Ethernet (PoE) injector and power cord.
- QR code card for C410 and C420 Quick Start and C410 and C420 User Guide.



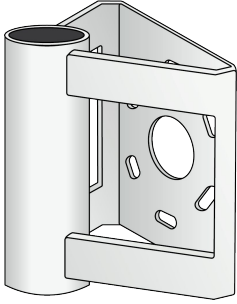
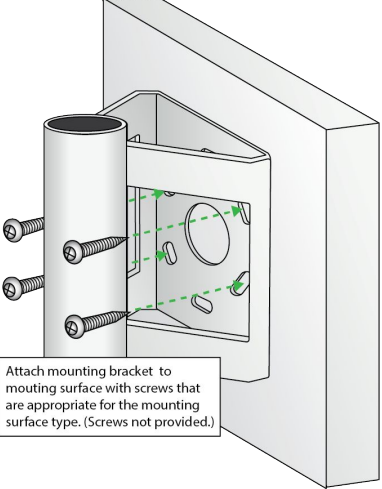
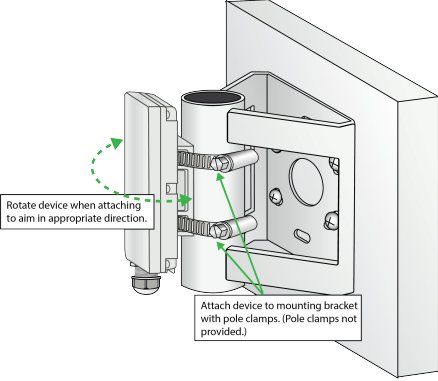
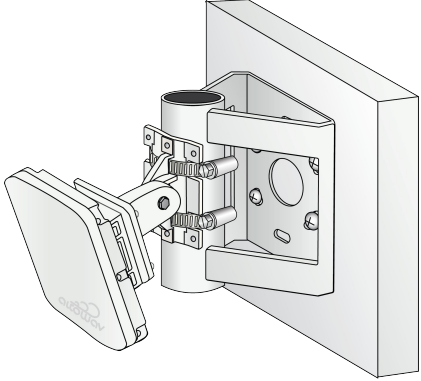
Mounting brackets

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.

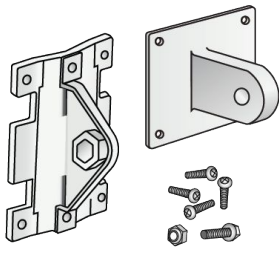
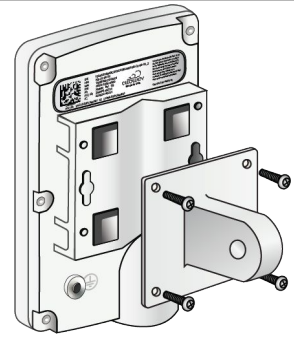
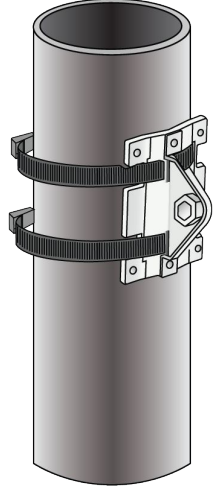
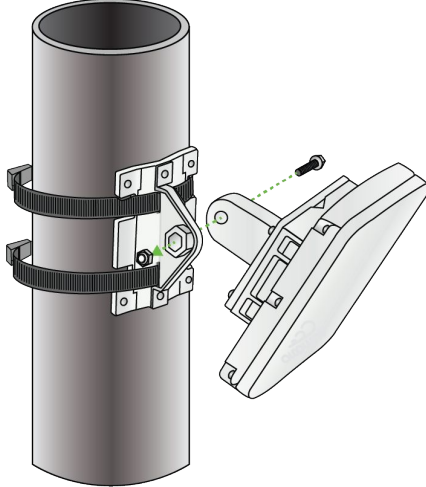
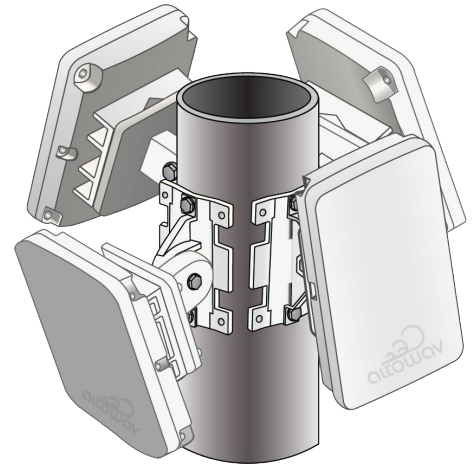
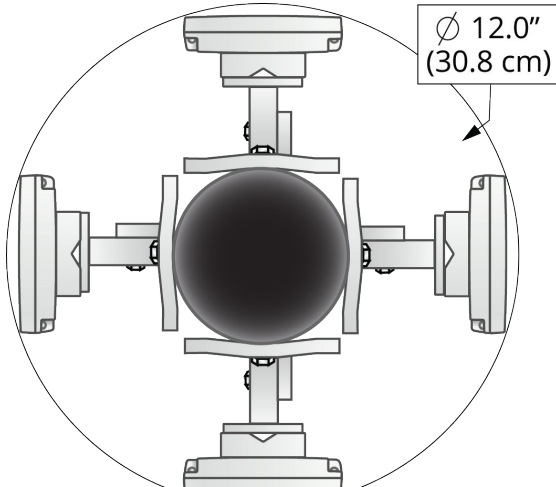
Altoway Wall Mount

The Altoway Wall Mount, model number AX-AW3-MT-WALL, can be used to securely mount the C410/C420 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
	 <p>Attach mounting bracket to mounting surface with screws that are appropriate for the mounting surface type. (Screws not provided.)</p>
Attach the C410/C420 to wall mount	Optional installation with the AltoPlex Extended Range Pole Mount
 <p>Rotate device when attaching to aim in appropriate direction.</p> <p>Attach device to mounting bracket with pole clamps. (Pole clamps not provided.)</p>	

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 C410/C420
	
Pole mounting with band clamps	
	
360° coverage	Small form factor
	

About the C410 and C420

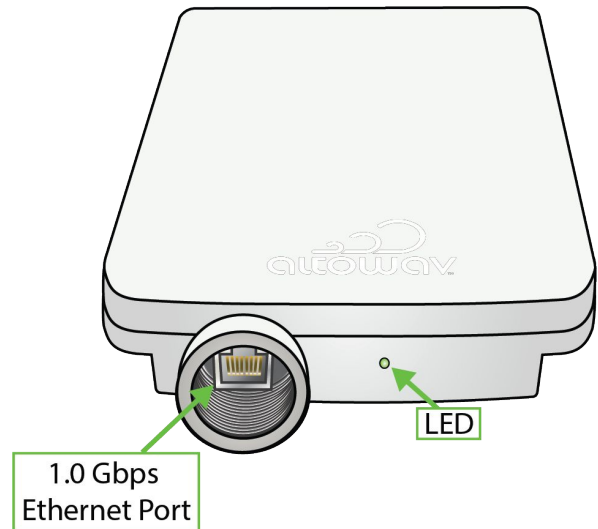
The C410 and C420 are client nodes (CNs) that work in tandem with the D621 distribution node (DN) to provide 60GHz wireless networking connectivity, giving fiber speeds at a fraction of the cost and with rapid deployment. Both models have the same durable and weatherproof outer case.

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

The red/green LED on the bottom of the C410/C420 device shows power, connection and activity.

- Red — powering up.
- Flashing red and green — during boot up.
- Flashing green — until at least one wired link and one wireless link is formed.
- Steady green — normal operations with one or more wired and one or more wireless link.

See [LED Indicators](#) for more detail.



Requirements for deployment

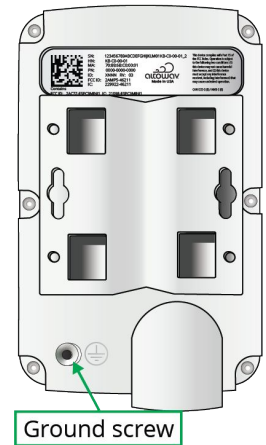
These items are required to form a wireless link with an AltoPlex device that is running in distribution node (DN) role:

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

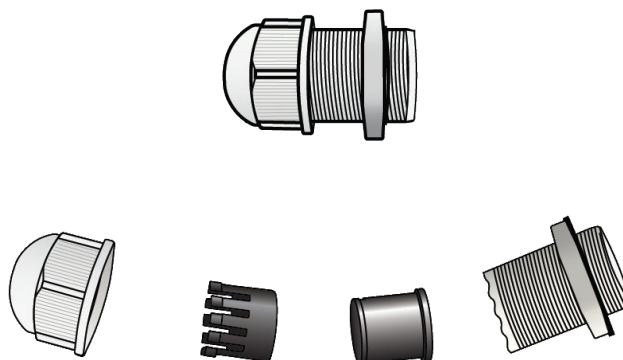
Installation steps

C410 and C420 devices are designed to work out of the box and should not need bench configuration prior to installation and connection.

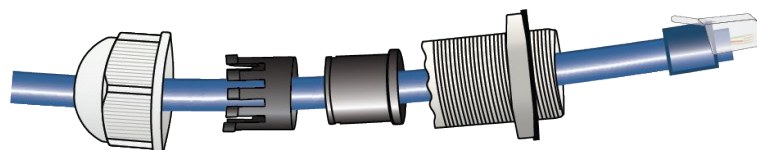
1. Install the ground wire, if required by code, at the installation location. Connect the other end of the ground wire to nearby good earth. The ground screw on AltoPlex devices is a #6-32 5/16th inch Phillips head screw.



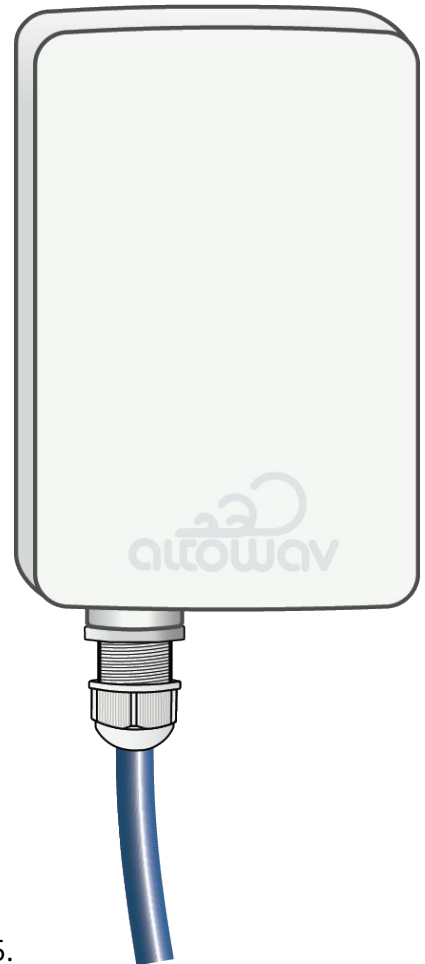
2. Install an outdoor-rated Ethernet cable through the provided cable gland and into the port on the C410/C420 device:
 - A. Unscrew and deconstruct the components of the gland.



- 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. 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 C410 and C420 according to the planned azimuth and elevation.
4. PoE options available from Altoway include:
 - Outdoor PoE switch, part number AX-PSWOD-4AT-4C25.
 - Outdoor PoE switch mounting bracket, part number AX-PSW-OD-MOUNT.
5. Connect the other end of the Cat5e cable to the PoE port on the PoE injector or to a PoE switch.

Note: The supplied PoE injector is an indoor unit so it requires a weatherproof box for outdoor installation.

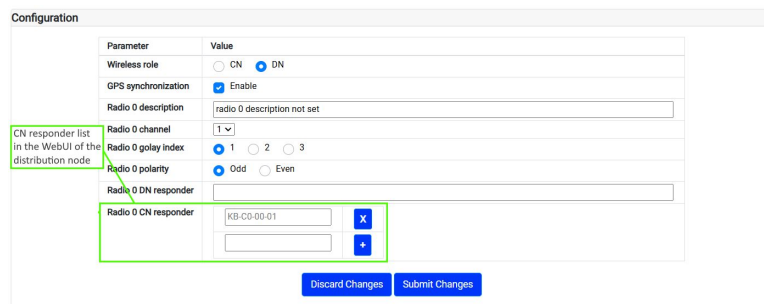
6. Verify that the device powers up. (LED is red during boot-up and then flashing green.)



Add the C410/C420 as a client node to a distribution node

The C410/C420 can only operate as a client node (CN) that is attached to a distribution node (DN). This connection is configured on the distribution node after the client node has been installed. This section describes how to add the C410/C420 to a distribution node and complete and verify the installation.

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



The screenshot shows the 'Configuration' page with the following parameters and values:

Parameter	Value
Wireless role	<input type="radio"/> CN <input checked="" type="radio"/> DN
GPS synchronization	<input checked="" type="checkbox"/> Enable
Radio 0 description	radio 0 description not set
Radio 0 channel	1
Radio 0 golay index	<input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3
Radio 0 polarity	<input checked="" type="radio"/> Odd <input type="radio"/> Even
Radio 0 DN responder	
Radio 0 CN responder	KB-C0-00-01 <input type="button" value="X"/> <input type="button" value="+"/>

Buttons:

The wireless link is formed with no further configuration on the C410 and C420 device, provided that:

- The line of sight to the distribution node is clear.
 - The distance to the distribution node is up to 300 meters for a C420 or 200 meters for a C410.
 - Network settings for Management VLAN are the same for both devices. The factory defaults work for this.
2. After the device connects, review and configure its settings. With the wireless link active, this can be done remotely. [C410/C420 Configuration via WebUI](#) provides options for how to access the C410 and C420 WebUI.
 - A. Set the **Location** and **Description** on the **Admin** tab.
 - B. Review settings on the **LAN** and **Network** tabs and adjust as required.
 3. Verify the operation of the new device and review its performance. Adjust for line of sight, and rebeamform as needed. Dress the cable and power cord securely to avoid wear.

Connecting to the C410 and C420

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

Additionally:

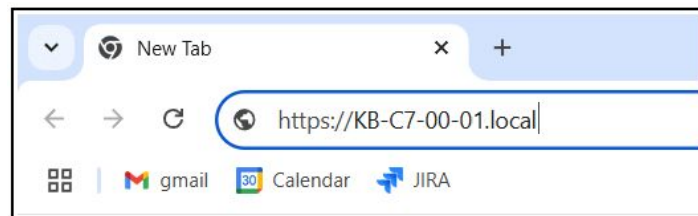
- Radios can be configured to use a static IP address, rather than dynamic IP address assignment. This will override the fallback IP unless the radio is [factory reset](#). After a factory reset, it will return to default behavior.
- Radios upgraded to release 3.6.0 that have not been factory reset will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

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

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

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

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



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

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

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

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

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

For example, on Windows 11:

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

2. Next, either:

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

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

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

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

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

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

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

The WebUI will open with the [Status tab](#) displayed.

Determine the IP address of a radio by using mDNS

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

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

- Windows Powershell:
`Resolve-DnsName <hostname>`
- MacOS:
`dns-sd -G v4v6 <hostname>`
- Linux:
`avahi-resolve-host-name -4 <hostname>.local`

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

C410/C420 Configuration via WebUI

During installation, the hostname (KB-XX-XX-XX) of the C410/C420 device is added to the **CN responder** list for the specific distribution node (DN) device to which it connects. That configuration change for the distribution node initiates the wireless link between the the distribution node and the C410/C420 client node.

After the C410/C420 link to the network is active, you can access the WebUI using one of the following methods:

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



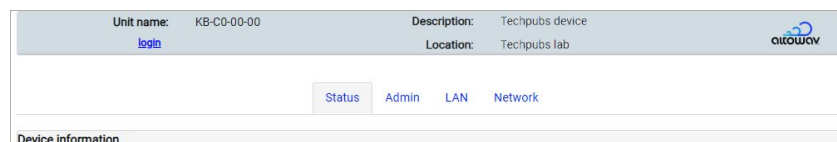
Radio	MAC Address	Description	Chan	DN/ CN	Peer-Name	State	Link Uptime	SNR	RSSI	TX MCS	TX Power Index	TX angles	R/D ar
0	70:88:6b:c0:00:00	radio 0 description not set	2	CN	KB-C0-00-01	UP	0 days 00:13:22	12/20	-62/-54	10/9	6/8	-3.5/0 -24.5/7.5	1/2

- Access the WebUI of the C410/C420. 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 C410 and C420](#) for more information.
- If using the AltoCommand web-based management tool, access the WebUI from the **Devices** page. On the row of the device to configure, click the menu icon (☰) in the settings (⚙️) column and click **Connect to Device**.

General startup configuration steps for the C410/C420 often include:

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

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




Status tab

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

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

Description: Techpubs device
Location: Techpubs lab



Status
Admin
Wireless
LAN
Network

Device information

Device model:	C410
Device role:	CN
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:	
Latitude	44.8608139 degrees
Longitude	-93.3608598 degrees
Altitude	283.846 meters
Device Temperature:	No temperature sensor on this unit

Wireless

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:C0:00:00	UP	4	00:00:00:00:00:00	KB-00-00-00	16/13	-58/-61	10/10	6/6

LAN interfaces

Interface number	1
Enabled:	Yes
Status:	Not connected
Duplex:	N/A
Speed:	N/A
Maximum supported speed:	2.5 Gb/s
Power Over Ethernet:	Input
LL Discovery:	KB-C7-00-01 KB-C7-00-02

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

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

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

Status tab — Wireless

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

Status tab — LAN interfaces section

This section shows information for the LAN interface (Port 1 for the C410 and C420), including whether the port is enabled, its status (**Connected** or **Not connected**), duplex mode, speed, maximum supported speed, and PoE mode.

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

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

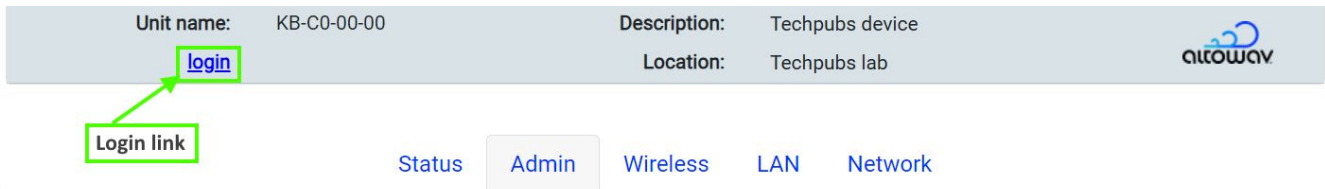
Status tab — Management interface

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

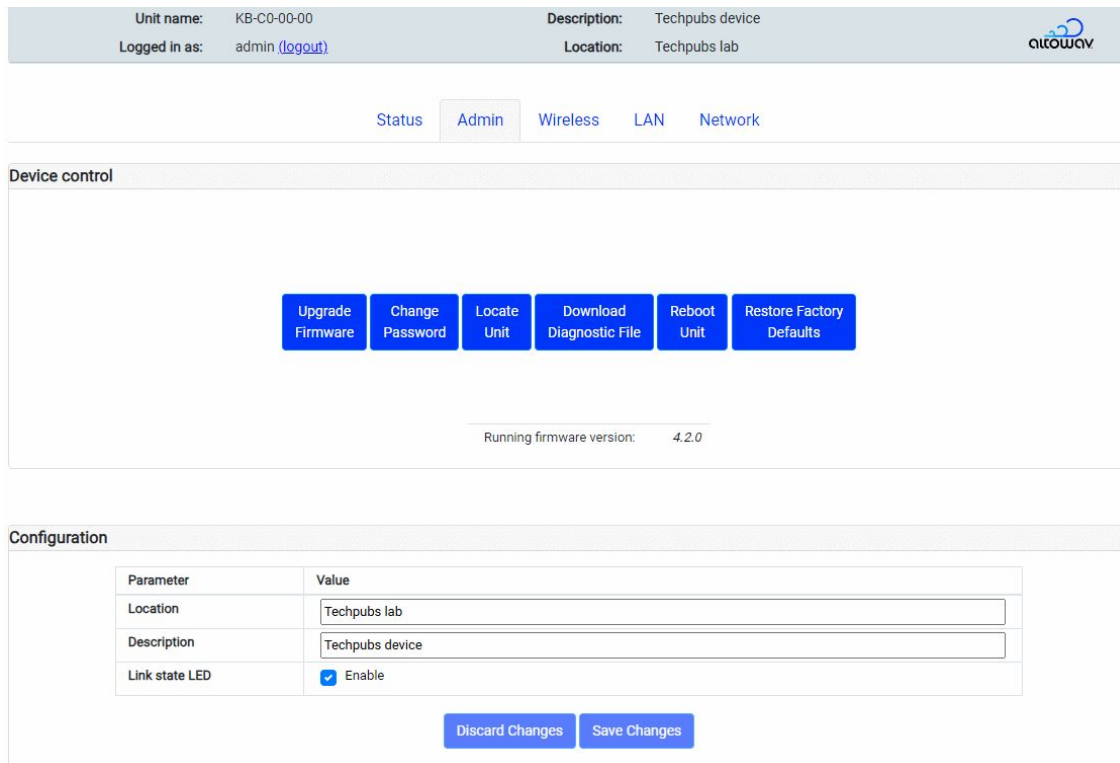
Admin tab

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

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



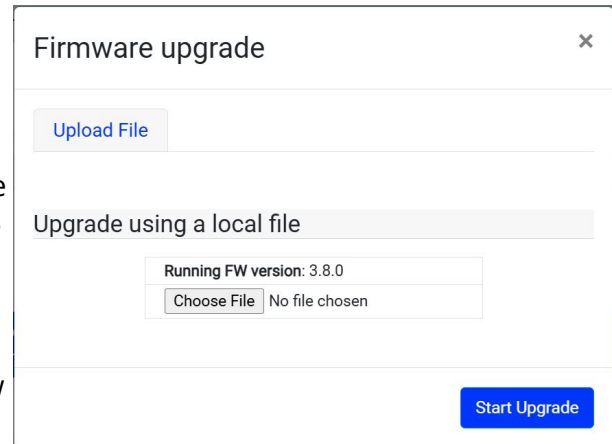
The **Admin** tab has two sections: **Device control** and **Configuration**.



Admin tab — Device control section

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

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



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 C410 and C420. 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](#).

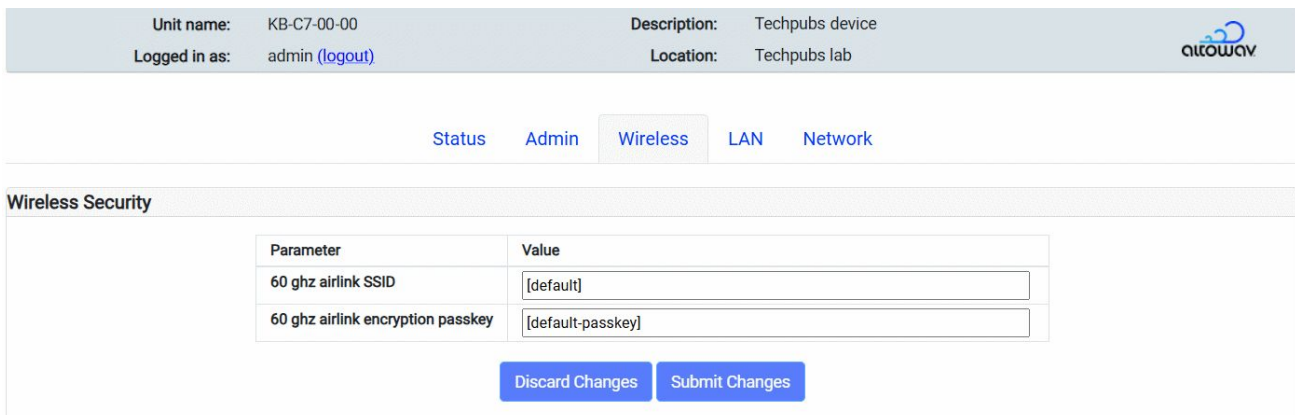
Wireless tab

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

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

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

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

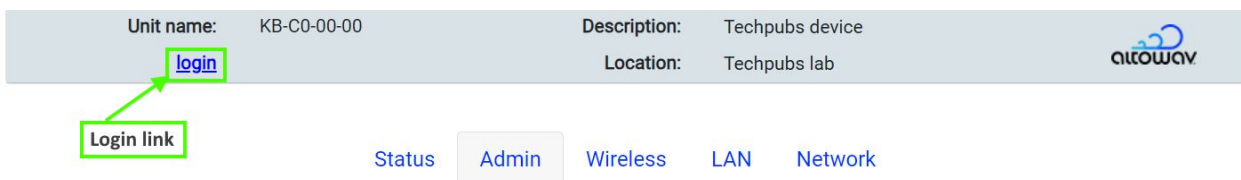


Parameter	Value
60 ghz airlink SSID	[default]
60 ghz airlink encryption passkey	[default-passkey]

Discard Changes Submit Changes

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**.



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

[login](#)

Login link

Status Admin Wireless LAN Network


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.

Network tab

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

Note: Adding a C410/C420 device's hostname (KB-XX-XX-XX) to the **CN responder** list in a distribution node's (DN) configuration initiates the wireless link between the DN and the C410/C420. These devices are designed to work with other AltoPlex devices out of the box.

Unit name: KB-C0-00-00 Description: Techpubs device
Logged in as: admin ([logout](#)) Location: Techpubs lab



Status Admin Wireless LAN Network

Network Reachability Configuration

– Management Network Interface Configuration –

Parameter	Value
IP assignment method	<input type="radio"/> Static <input checked="" type="radio"/> Dynamic
IP address (static)	<input type="text" value="192.168.0.51"/>
Network mask (static)	<input type="text" value="255.255.0.0"/>
Network gateway (static)	<input type="text" value="192.168.0.1"/>

– Virtual LAN Configuration –

Parameter	Value
VLAN 802.1q mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Management 802.1q VLAN ID	<input type="text" value="1"/>
Ethernet port 1 802.1q accepted frame types	<input checked="" type="radio"/> All <input type="radio"/> Tagged
Ethernet port 1 802.1q PVID	<input type="text" value="1"/>
Ethernet port 1 802.1q membership	<input type="text" value="1"/> X <input type="text"/> +

– Port Isolation –

Parameter	Value
Ethernet port 1 isolation	<input type="checkbox"/> Enable
Wireless port isolation	<input type="checkbox"/> Enable

Discard Changes
Submit Changes

Network tab — Network Reachability Configuration

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

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

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

Network tab — Spanning Tree Protocol Configuration

Spanning Tree Protocol Configuration

Parameter	Value
Spanning tree protocol (stp) enable	<input type="checkbox"/> Enable
STP bridge priority	<input style="width: 100px;" type="text" value="8"/>
STP radio 0 port path cost	<input style="width: 100px;" type="text" value="20000"/>
STP Ethernet port 1 bpdu filter	<input type="checkbox"/> Enable

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	<input checked="" type="checkbox"/> Enable
SNMP read-only community	<input type="text" value="public"/>
SNMPv2 notification enable	<input type="checkbox"/> Enable
SNMPv2 notification community	<input type="text" value="public"/>
SNMPv2 notification destination	<input type="text" value="localhost"/>
SNMPv2 notification port	<input type="text" value="162"/>

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	<input type="text"/>

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 C410/C420's Ethernet port, in ASCII format), or the **Hostif** (the hostname:Ethernet_port of the C410/C420 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	<input type="checkbox"/> Enable
DHCP relay agent circuit ID type	<input checked="" type="radio"/> Hwaddr <input type="radio"/> Hostif
Ethernet port 1 host access	<input checked="" type="radio"/> Trusted <input type="radio"/> Untrusted

[Discard Changes](#) [Submit Changes](#)

Maintenance and security

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.

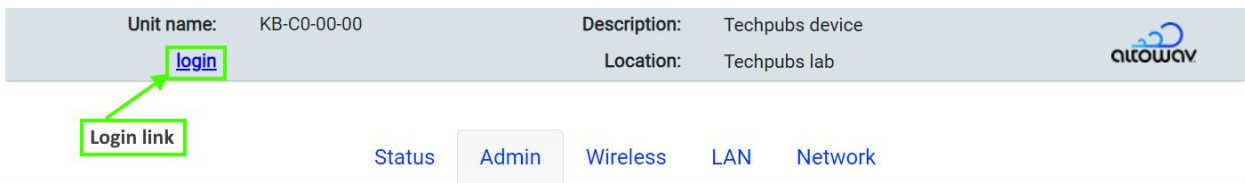
To change the device password:

1. Access the WebUI of the C410/C420. In your browser's address bar, type:

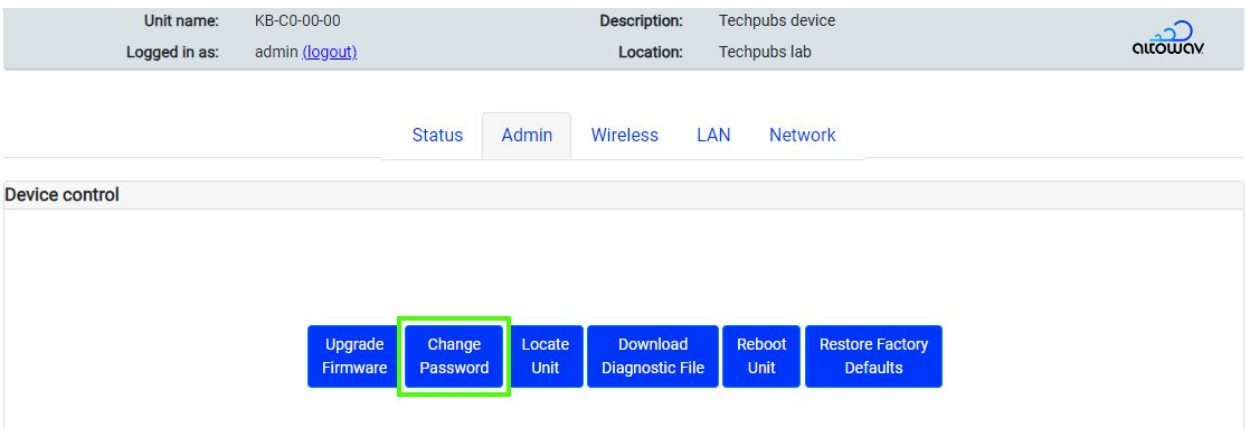
https://hostname

where *hostname* is the hostname (KB-XX-XX-XX) or IP address of the radio. See [Connecting to the C410 and C420](#) 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 C410/C420 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 C410/C420.

Note: This procedure describes how to upload an SSH key to the C410 and C420. 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 C410/C420:

```
$ 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 C410 and C420](#) 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.altoway.com) at support.altoway.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.altowav.com) at support.altowav.com.

The following files are included in the firmware zip file:

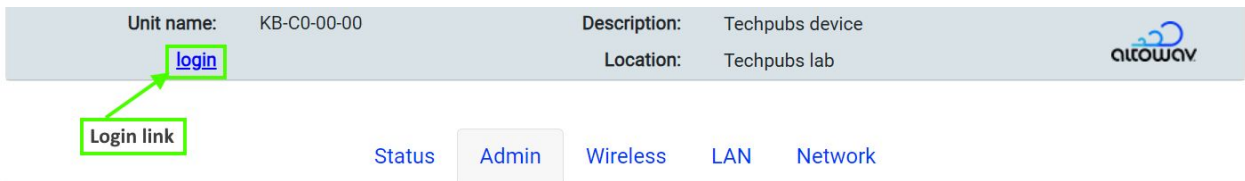
- A digest file, not used as part of this upgrade process.
- The firmware binary. See The upgrade software filename for information about the filename used for the firmware binary.

2. Access the WebUI of the C410/C420. In your browser's address bar, type:

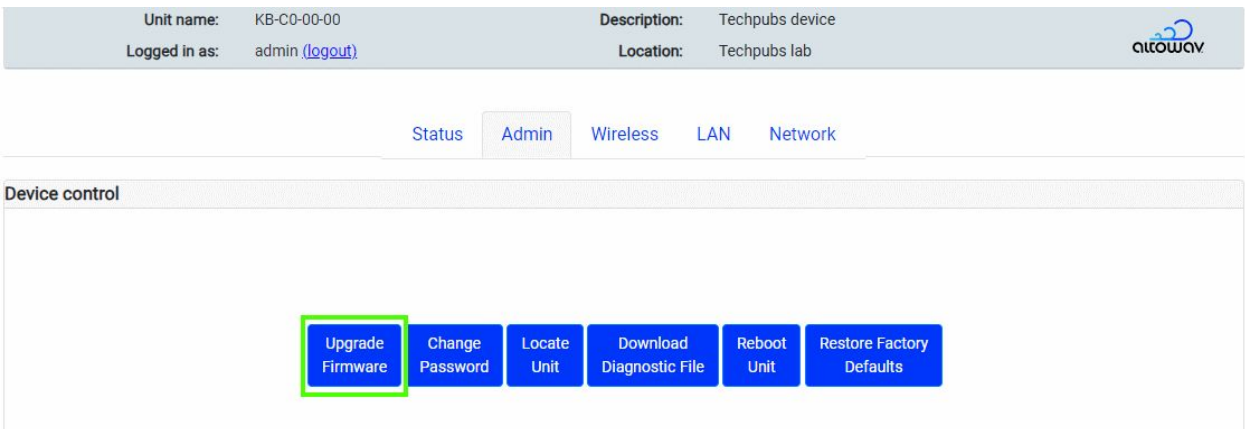
https://hostname

where *hostname* is the hostname (KB-XX-XX-XX) or IP address of the radio. See [Connecting to the C410 and C420](#) for more information.

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

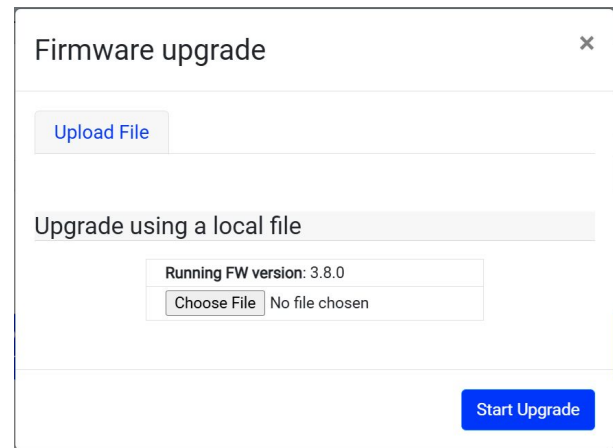


4. Click the **Admin** tab.
5. Click the **Upgrade Firmware** button.



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 C410/C420 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 C410/C420:

```
$ 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 C410 and C420](#) 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 C410/C420. 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 C410/C420:

```
$ 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 C410 and C420](#) 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 C410/C420. 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.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 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
{
```

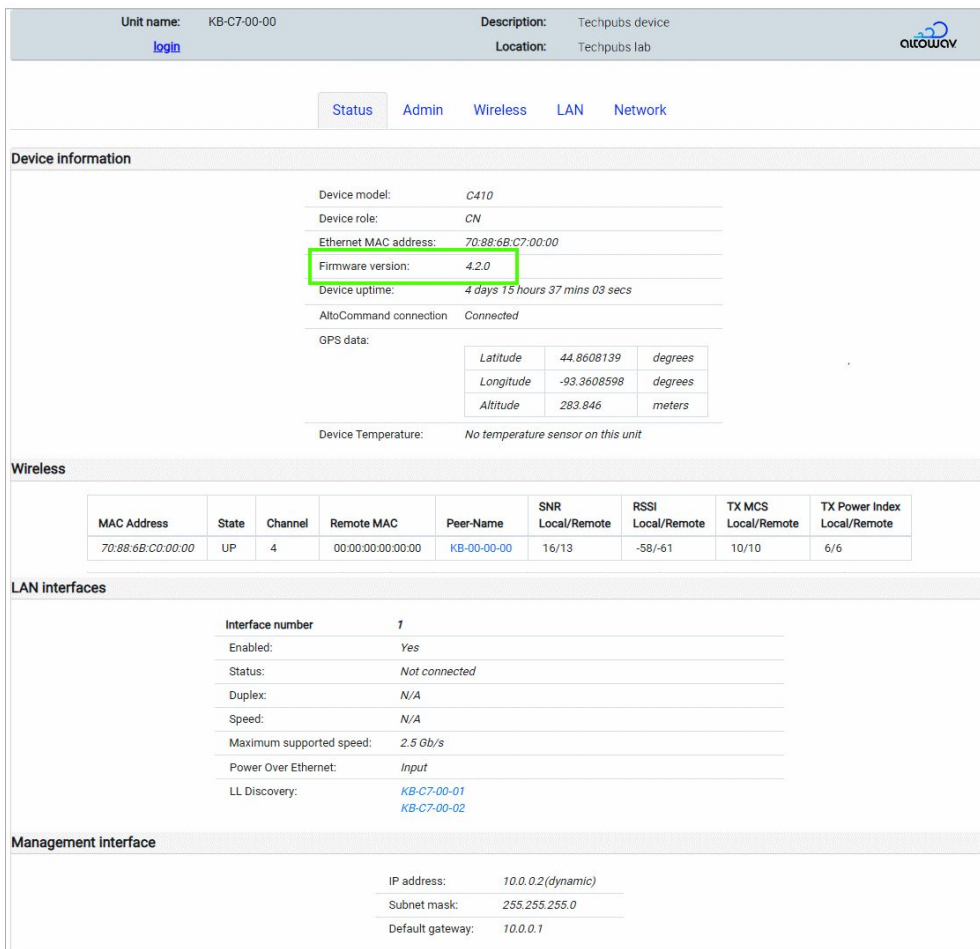
```
"status": "starting",
"running-sw-version": "3.9.1",
"upgrade-running": "yes"
}
```

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 device. At the top, there is a header with 'Unit name: KB-C7-00-00', 'Description: Techpubs device', 'Location: Techpubs lab', and a 'login' link. Below the header are tabs for 'Status', 'Admin', 'Wireless', 'LAN', and 'Network'. The 'Status' tab is selected, and the 'Device information' section is expanded. The 'Firmware version' is highlighted with a green box and shows '4.2.0'. Other fields include 'Device model: C410', 'Device role: CN', 'Ethernet MAC address: 70:88:6B:C7:00:00', 'Device uptime: 4 days 15 hours 37 mins 03 secs', 'AltoCommand connection: Connected', and 'GPS data' (Latitude: 44.8608139 degrees, Longitude: -93.3608598 degrees, Altitude: 283.846 meters). Below this is the 'Wireless' section with a table of wireless connections. The 'LAN interfaces' section shows interface 1 with details like 'Enabled: Yes', 'Status: Not connected', 'Speed: N/A', and 'Maximum supported speed: 2.5 Gb/s'. The 'Management interface' section shows 'IP address: 10.0.0.2 (dynamic)', 'Subnet mask: 255.255.255.0', and 'Default gateway: 10.0.0.1'.

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:C0:00:00	UP	4	00:00:00:00:00:00	KB-00-00-00	16/13	-58/-61	10/10	6/6

Verify firmware update from the command line

1. Log in via ssh to the C410/C420:

```
$ 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 C410 and C420](#) for more information.

2. Enter **control** mode:

```
KB-C7-00-01> control
KB-C7-00-01(control)>
```

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

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

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

Verify firmware update from the REST API

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

```
$ curl -k -u admin:admin https://KB-C7-00-01/rest/v002/device/node_identity
% Total    % Received % Xferd  Average Speed   Time    Time     Time
Current                        Dload  Upload  Total   Spent    Left
Speed
100 605  100  605    0    0  8188      0 --:--:-- --:--:-- --:--:--
8402{
  "Ethernet MAC" : "70:88:6B:C7:00:01",
  "HW name" : "devo",
  "HW rev" : 2,
  "HW type code" : 82,
  "Node role" : "CN",
  "Number Ethernet Interfaces" : 1,
  "Number RF Interfaces" : 1,
  "Part number" : "1900-8411-1012-devo-2-LBKA0ZZ1SV1",
  "Serial number" : "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

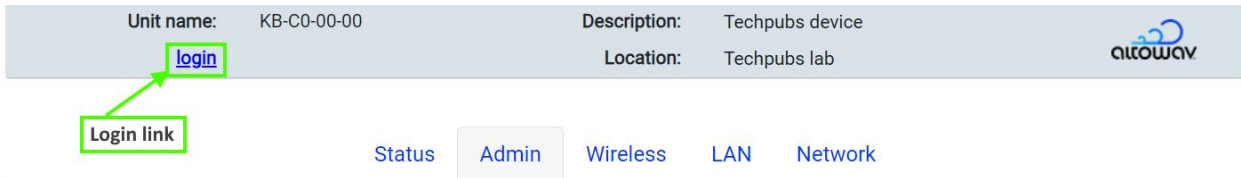
Note: A power-cycle or reboot clears the diagnostic log information stored in the device. So during troubleshooting, you should capture the diagnostic log in a file, before the power-cycle or reboot. If you require troubleshooting assistance, information in the diagnostic log may be useful.

1. Access the WebUI of the C410/C420. In your browser's address bar, type:

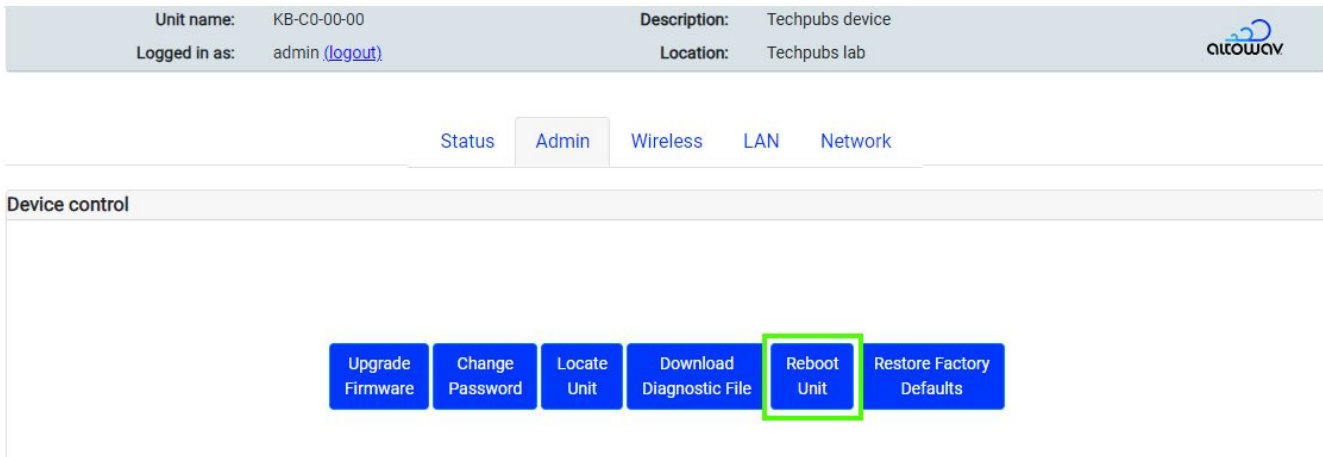
https://hostname

where *hostname* is the hostname (KB-XX-XX-XX) or IP address of the radio. See [Connecting to the C410 and C420](#) 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

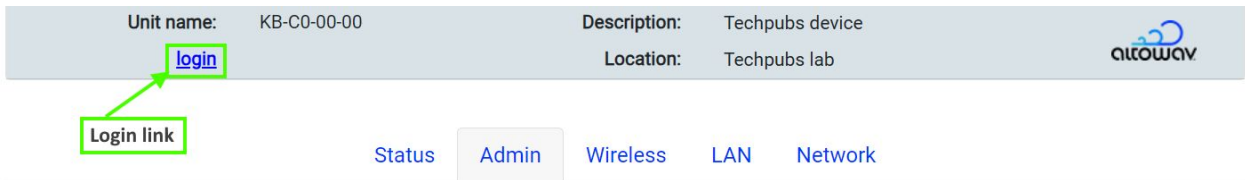
Use the **Restore Factory Defaults** button in the device's WebUI to reset the device.

1. Access the WebUI of the C410/C420. In your browser's address bar, type:

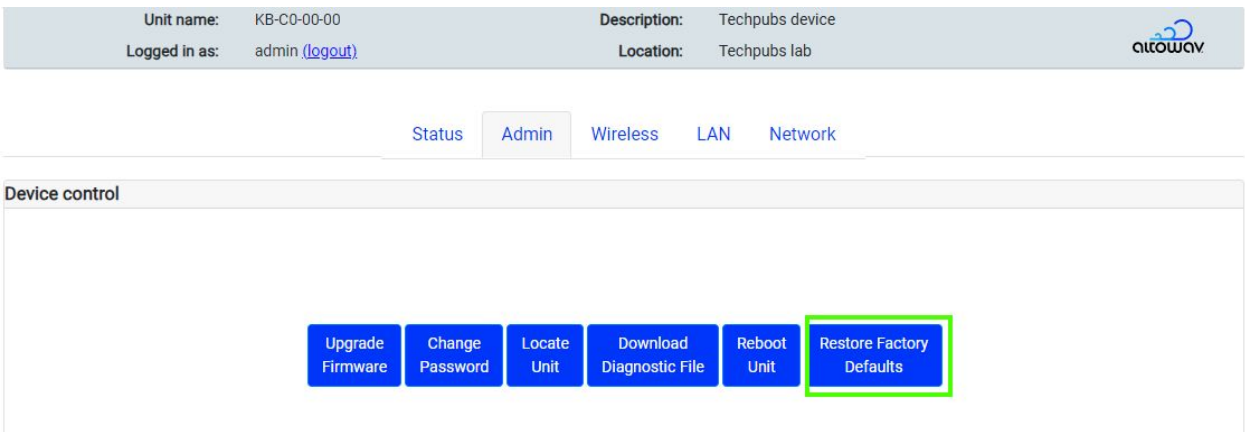
https://hostname

where *hostname* is the hostname (KB-XX-XX-XX) or IP address of the radio. See [Connecting to the C410 and C420](#) 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.



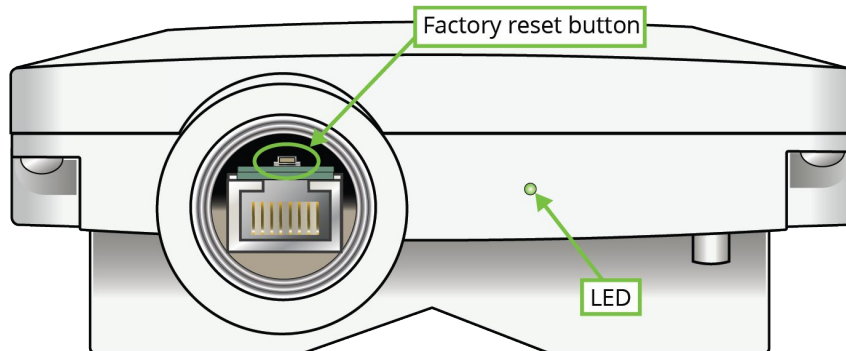
5. A confirmation dialog opens. Enter the text **confirm factory reset** and click **OK**.

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:





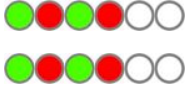
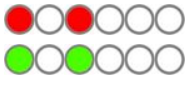
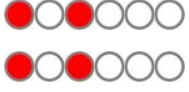
- [LED Indicators](#)
- [Lost Password](#)
- [Download a Diagnostic File](#)
- [MAC addresses used by the C410 and C420](#)

LED Indicators

The C410 and C420 is equipped with a single LED, showing both red and green lights to indicate power, connection and activity.



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

LED behavior		Indicates
	Solid red	Device is powering up.
	Flashing green	Device is waiting to form a wired connection and at least one wireless connection.
	Solid green	Device has a wired connection and at least one wireless connection.
	Flashing red/green	Device is in locate mode.
	Flashing red/green, pausing, then flashing red/green again.	Device is booting and ready for the factory reset button to be pressed. The device will stay in this mode for approximately ten seconds, or until the factory reset button is pressed. See Factory Reset for information about performing a factory reset.
	Flashing red, pausing, then flashing green, pausing, then repeating.	The factory reset button has been pressed and the device is performing a factory reset .
	Flashing red, pausing, then repeating.	Error condition.

Lost Password

If a C410 and C420 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

Altoway 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@altoway.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.

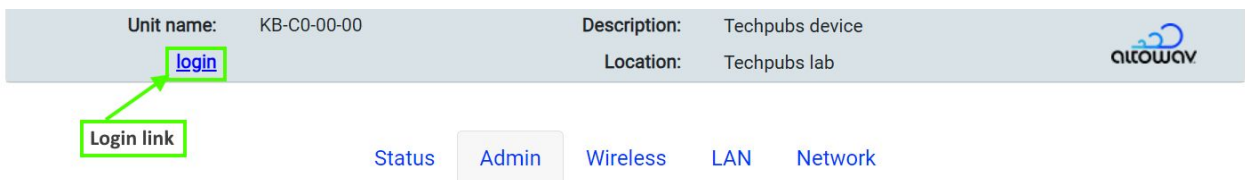
Follow these steps to download a diagnostic file for connected devices from the WebUI:

1. Access the WebUI of the C410/C420. In your browser's address bar, type:

`https://hostname`

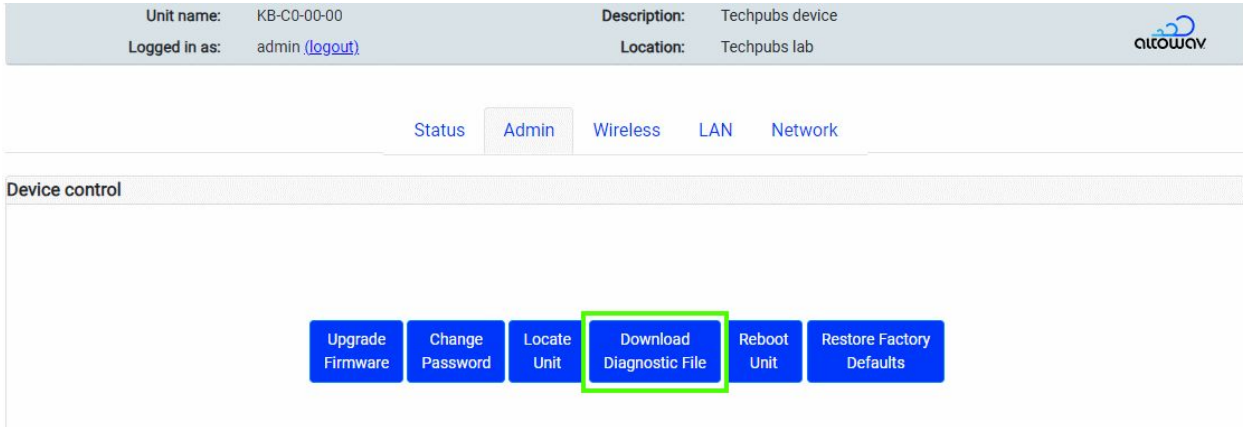
where *hostname* is the hostname (KB-XX-XX-XX) or IP address of the radio. See [Connecting to the C410 and C420](#) for more information.

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 C410 and C420

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 eth1 interface uses the same MAC address as wlan0, except incremented by one.	70:88:6B:C7:00:01

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.

