

## **Altoway AltoPlex Series C410 and C420 User Guide**

October 25, 2024

Version 3.0.0

## Copyright, trademark, and legal information

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE ARE PROVIDED "AS IS" WITH ALL FAULTS. ALTOWAV DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND 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 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 except for the conditions listed in 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, sauf dans les conditions énumérées dans ISDE RSS-210, annexe J.

## Revision history

Revisions	Version
Initial release of the C410 and C420.	10/25/2024

## Contents

<b>C410 and C420 User Guide overview</b> .....	<b>6</b>
Additional Documents.....	6
Additional help .....	6
<b>Introduction</b> .....	<b>7</b>
<b>C410/C420 installation and configuration</b> .....	<b>8</b>
Tool List: .....	8
Box contents .....	8
Mounting options.....	9
About the C410 and C420 .....	10
Requirements for deployment.....	10
Installation steps .....	11
C410/C420 Configuration via WebUI.....	14
<b>Maintenance and security</b> .....	<b>23</b>
Change a device password .....	23
Enable Passwordless SSH .....	25
Upgrade firmware.....	26
Reboot.....	34
Factory Reset .....	35
<b>Troubleshooting</b> .....	<b>37</b>
LED Indicators.....	38
Lost Password.....	39
Download a Diagnostic File.....	39
<b>Glossary</b> .....	<b>41</b>

## 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, see [altowav.com/technology/](https://altowav.com/technology/)
- [C410 and C420 Quick Start Guide.pdf](#)
- [D621 User Guide.pdf](#)
- [Altowav AltoCommand User Guide.pdf](#)
- 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	<a href="https://support.altowav.com">support.altowav.com</a>
-----	---

---

E-mail	<a href="mailto:support@altowav.com">support@altowav.com</a>
--------	--

---

## 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).
- Wireless GPON.
- Surveillance camera connectivity.
- Smart city / smart pole distribution.
- Garden-style multi-dwelling unit distribution.
- High-speed data offload.

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

## C410/C420 installation and configuration

The installation instructions for C410 and C420 devices include:

- Tool list.
- C410/C420 box contents and mounting options.
- 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

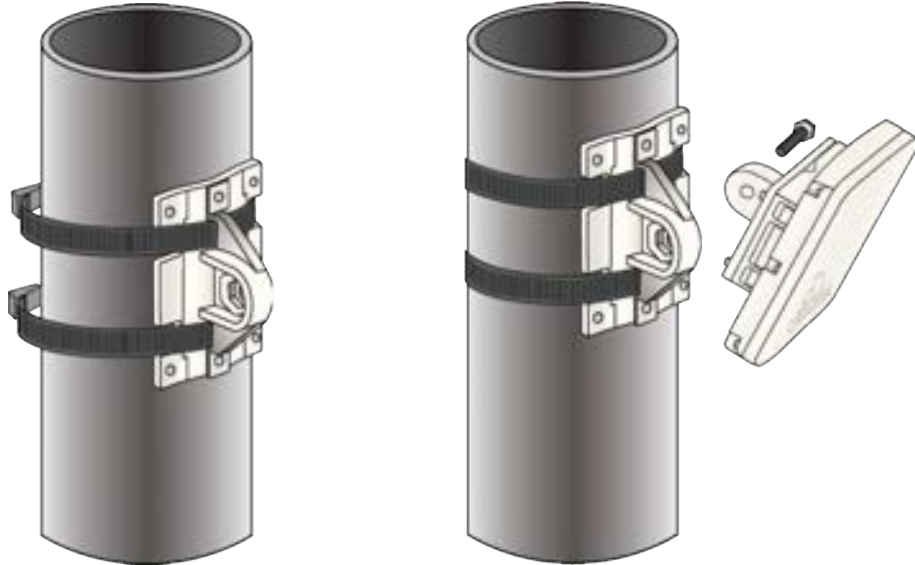
- C410/C420 device.
- IP67 cable gland.
- Indoor Power over Ethernet (PoE) injector:
  - Power supply for the C410:
    - Altowav part number: 1420-3016-0480
    - Vendor: Procet
    - Vendor number: AA01059
    - Vender model: EN15GF
  - Power supply for the C420 and P421:
    - Altowav part number: 1420-3017-0480
    - Vendor: Procet
    - Vendor number: AA01072
    - Vender model: EN30GT
  - Power cord.
- QR code card for C410 and C420 Quick Start and C410 and C420 User Guide.



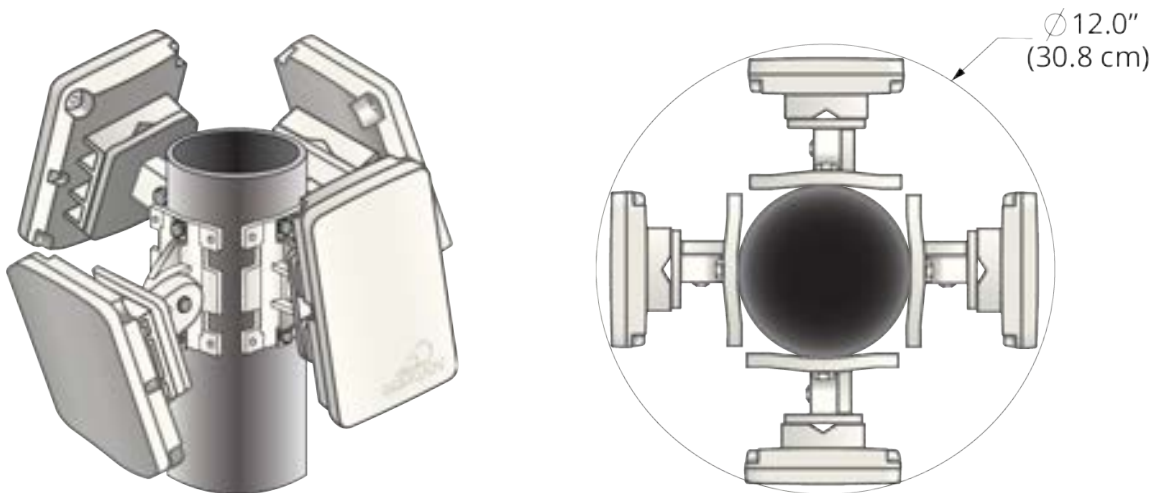


## Mounting options

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



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



## About the C410 and C420

The C410 and C420 are client nodes (CNs) supporting the AltoPlex platform for 60GHz wireless connectivity, providing fiber speeds at a fraction of the cost, and with rapid deployment. Both models have the same durable and weatherproof outer case.

The 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.



2. Install an outdoor-rated Cat5e cable in the port on the C410/C420 device:
  - A. Unscrew and deconstruct the components of the gland.



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



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



3. Mount the device to a wall or pole at the installation location with the mounting bracket (see Mounting options). Ensure a clear line of sight to the connecting distribution node.
4. Connect the other end of the Cat6 cable to the PoE port on the PoE injector. Connect the PoE injector to AC power. **Note**, the supplied PoE injector is an indoor unit so it requires a weatherproof box for outdoor installation.



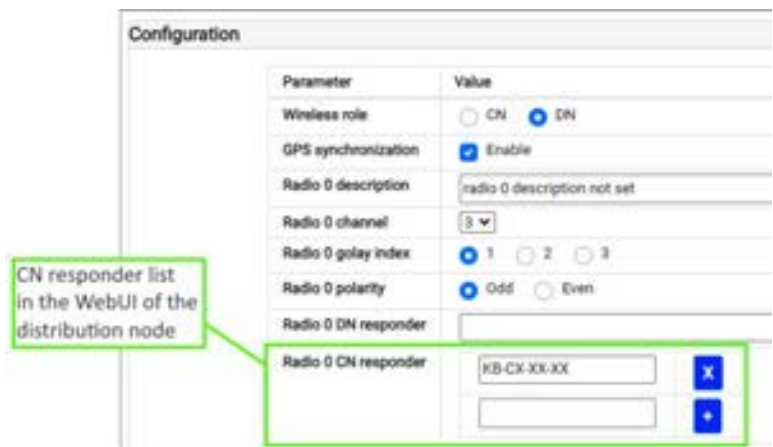
5. Verify that the device powers up. (LED is red during boot-up and then flashing green.)



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

The wireless link is formed with no further configuration on the 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.



7. 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.
8. 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.

## 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 connected distribution node's WebUI. Click on the device listed in the **Peer-Name** column.

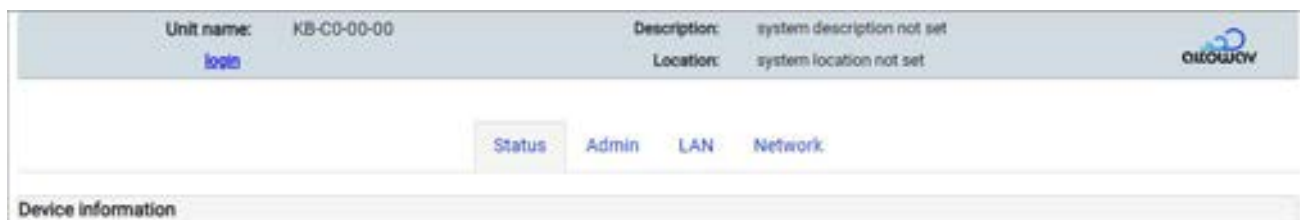
Wireless Status									
MAC Address	State	Channel	Remote MAC	Peer-Name	SNR Local/Remote	RSSI Local/Remote	TX MCS Local/Remote	TX Power Index Local/Remote	
ea:d4:7d:57:02:95	UP	4	83:09:7d:2d:6c:59	KB-C0-00-00	11/12	-63/-62	9/9	12/7	

- C410/C420 devices default to DHCP for IP assignment. Access the WebUI by browsing to the hostname or IP address. For example, if your network has a DHCP server and hostname resolution, type **https://<hostname>/** in the browser's address bar to access the WebUI for the device.
- 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:

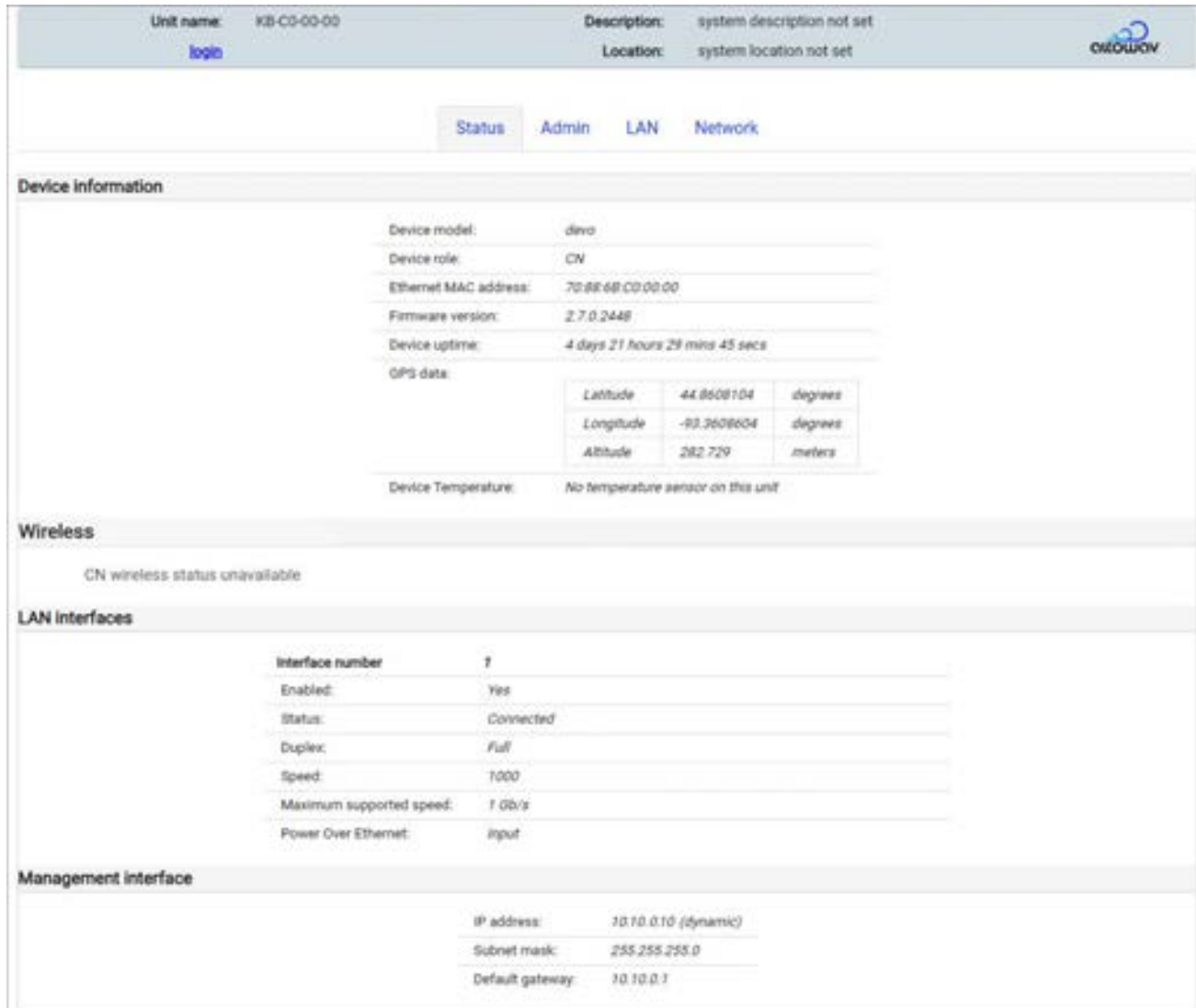
- Click on the **Admin** tab and do one or more of the following:
  - **Upgrade Firmware**
  - **Change Password**
  - Set the **Location**
  - Set the **Description**
- On Network tab, set network configuration items for the management network interface and VLAN.

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.



The screenshot shows the 'Status' tab of a device management interface. At the top, there is a header bar with 'Unit name: KB-C0-00-00' and a 'login' link. To the right, it shows 'Description: system description not set' and 'Location: system location not set'. Below this is a navigation menu with 'Status', 'Admin', 'LAN', and 'Network' tabs. The main content area is divided into several sections:

- Device information:**
  - Device model: divo
  - Device role: CN
  - Ethernet MAC address: 70:88:68:00:00:00
  - Firmware version: 2.7.0.2448
  - Device uptime: 4 days 21 hours 29 mins 45 secs
  - GPS data:
    - Latitude: 44.8508104 degrees
    - Longitude: -93.3608604 degrees
    - Altitude: 282.729 meters
  - Device Temperature: No temperature sensor on this unit
- Wireless:**
  - CN wireless status unavailable
- LAN interfaces:**
  - Interface number: 7
  - Enabled: Yes
  - Status: Connected
  - Duplex: Full
  - Speed: 1000
  - Maximum supported speed: 1 Gb/s
  - Power Over Ethernet: input
- Management interface:**
  - IP address: 10.10.0.10 (dynamic)
  - Subnet mask: 255.255.255.0
  - Default gateway: 10.10.0.1

## Device information

This area describes the model of the device, the device's role (CN — client node), Ethernet MAC address, firmware version, device uptime and GPS information.

## Wireless

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

## LAN interfaces

This area allows you shows information for the LAN interface: whether it is enabled, its status, duplex mode, speed, maximum supported speed, and PoE status.

## Management interface

This area 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

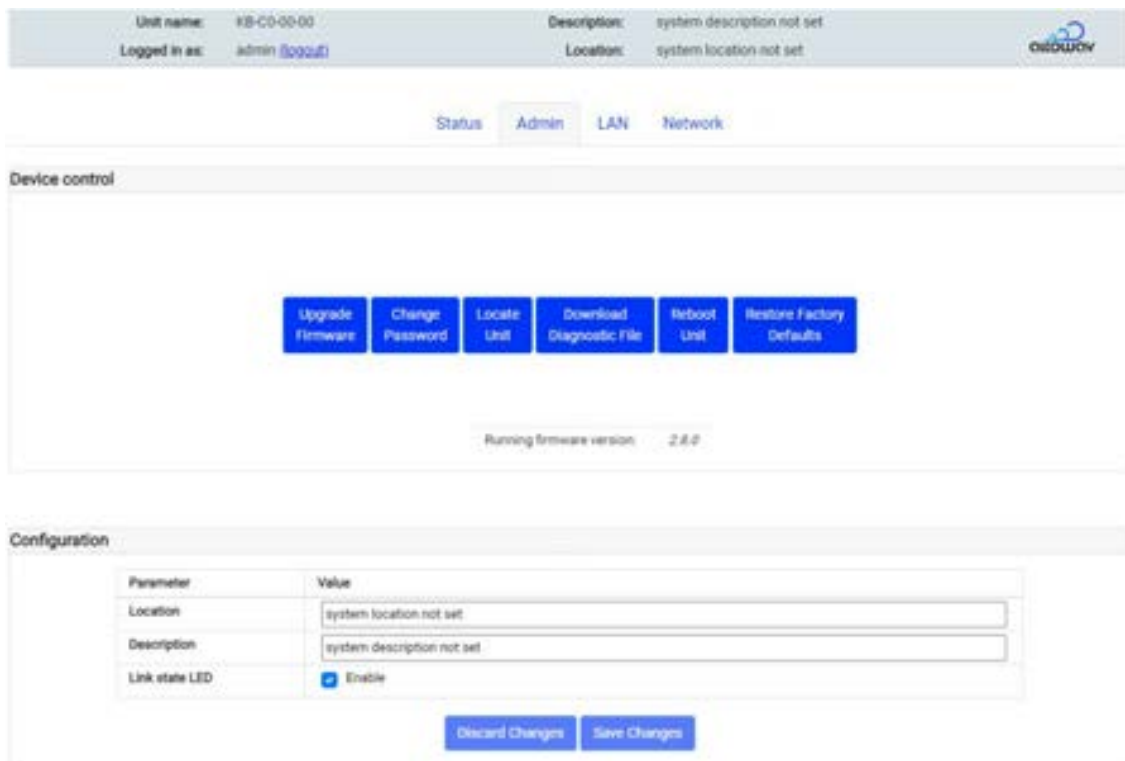
Unauthenticated users can view read-only information about the device in the WebUI. To make changes to the configuration, you must be logged in as an administrator.

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



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

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

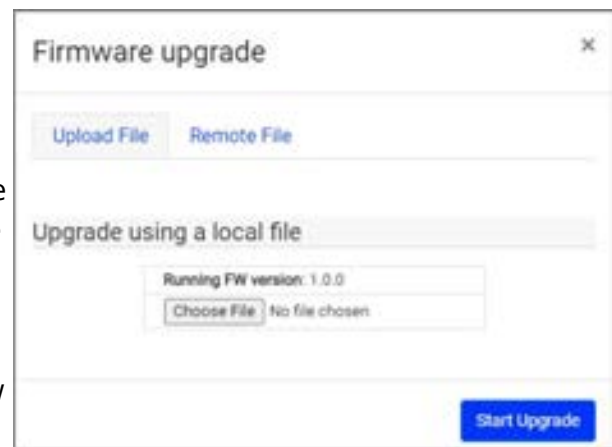


## Admin tab — Device control section

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

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



**Change Password** — Use this button to change the password for the admin of the C410 and C420.

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

**Download Diagnostic File** — Automatically downloads a detailed diagnostic text file for the device. The file contains detailed information about the device and its status at the time of the download. The file name includes the hostname, the date and time. For example, a file named KB-C0-00-01\_diag\_2024-10-25-14-43-32.txt, means this is the diagnostic text file for the device KB-C0-00-01, created at 2:43:32 pm (UTC) on October 25, 2024.

**Reboot Unit** — Restarts the unit remotely.

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

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

## Admin tab — Configuration section

This section includes the following settings:

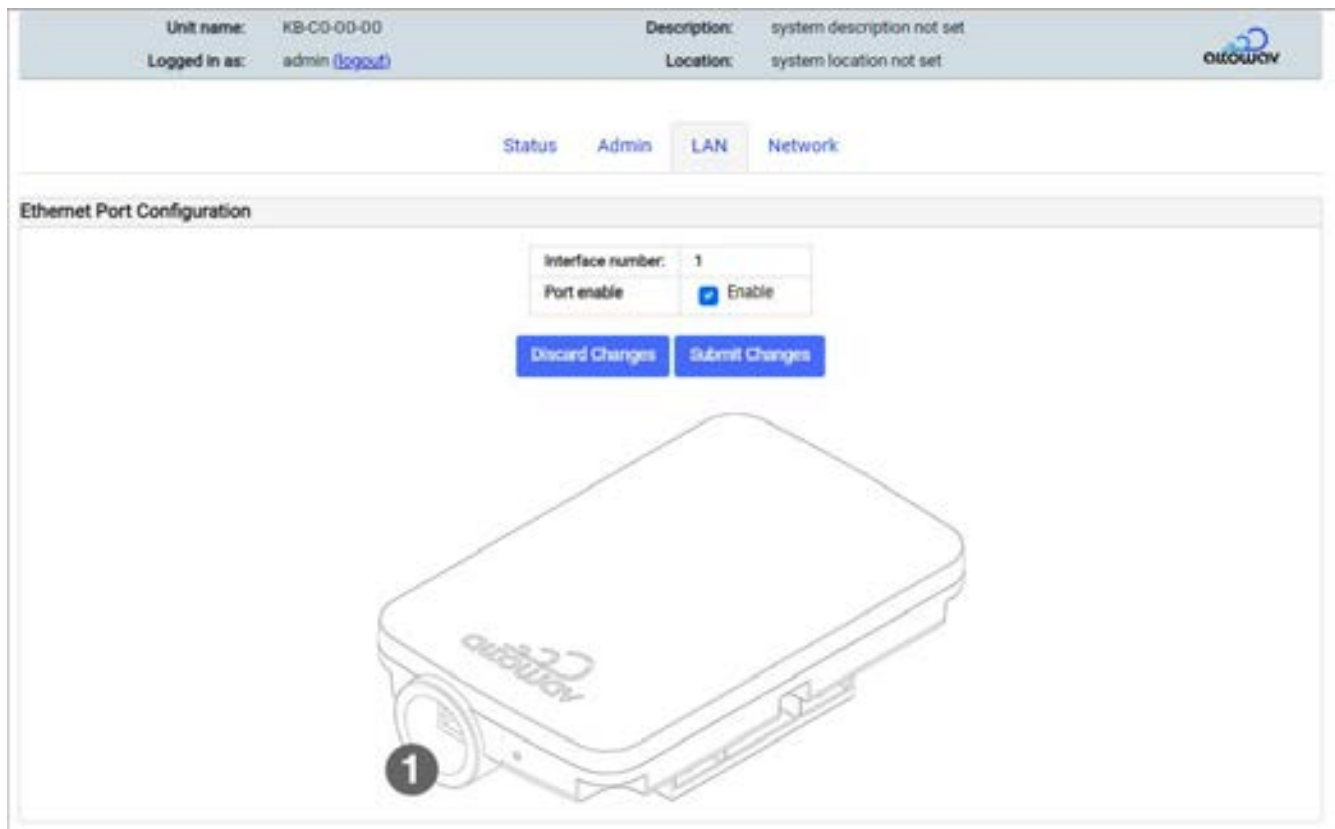
**Location** — Indicates the physical location where the device will be installed.

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

**Link state LED** — Enables or disables the LED for displaying the node status. See [LED indicators](#).

## LAN tab

The LAN tab provides settings for enabling Ethernet traffic on the LAN port for the C410/C420.



## Ethernet Port Configuration

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

The port is enabled by default.

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


## Network tab

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

Description: system description not set  
Location: system location not set



Status Admin 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"/> <span style="float: right; border: 1px solid #ccc; padding: 2px 5px;">X</span> <input type="text"/> <span style="float: right; border: 1px solid #ccc; padding: 2px 5px;">+</span>

– Port Isolation –

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

Discard Changes
Submit Changes

## Network Reachability Configuration

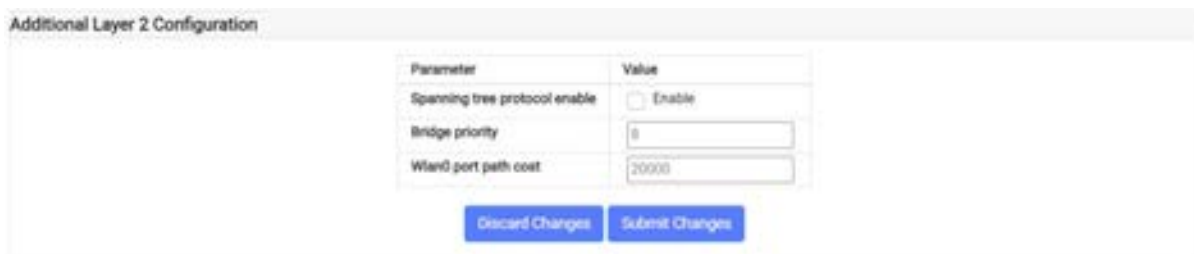
**Management Network Interface Configuration** — IP assignment method is Dynamic by default. If set to **Static**, the IP address, network mask and network gateway must set.

**Note:** If you set the IP address to **Static** and then lose or forget the IP address, the device will be unreachable, and you will need to [restore factory defaults by using the factory reset button](#).

**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.

## Additional Layer 2 Configuration



Parameter	Value
Spanning tree protocol enable	<input type="radio"/> Enable
Bridge priority	<input type="text" value="0"/>
Wired port path cost	<input type="text" value="20000"/>


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.

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

## SNMP Configuration



Parameter	Value
SNMP agent enable	<input checked="" type="radio"/> Enable
SNMP read-only community	<input type="text" value="public"/>
SNMPv2 notification enable	<input type="radio"/> 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"/>

Discard Changes Submit Changes

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.

## Network Services Configuration




The screenshot shows a web interface titled "Network Services Configuration". It contains a table with two columns: "Parameter" and "Value". The "Parameter" column has the entry "DNS IP list". The "Value" column is an empty text input field. Below the table are two buttons: "Discard Changes" and "Submit Changes".

Parameter	Value
DNS IP list	<input type="text"/>

**DNS IP list** — IP addresses for domain name servers (DNS) in dotted decimal format. This defaults to blank. If entering more than one IP address, separate them with commas.

## DHCP Relay Configuration (Option 82)



The screenshot shows a web interface titled "DHCP Relay Configuration (Option 82)". It contains a table with two columns: "Parameter" and "Value". The "Parameter" column has three entries: "DHCP relay agent enable", "DHCP relay agent circuit ID type", and "Ethernet port 1 host access". The "Value" column has three entries: "Enable" (with an unchecked checkbox), "Invisible" (with a checked radio button) and "Host" (with an unchecked radio button), and "Trusted" (with a checked radio button) and "Untrusted" (with an unchecked radio button). Below the table are two buttons: "Discard Changes" and "Submit Changes".

Parameter	Value
DHCP relay agent enable	<input type="checkbox"/> Enable
DHCP relay agent circuit ID type	<input checked="" type="radio"/> Invisible <input type="radio"/> Host
Ethernet port 1 host access	<input checked="" type="radio"/> Trusted <input type="radio"/> Untrusted

The DHCP relay agent (option 82) provides additional security when using DHCP. Enabling this option can prevent unauthorized contact with the DHCP server.

## Maintenance and security

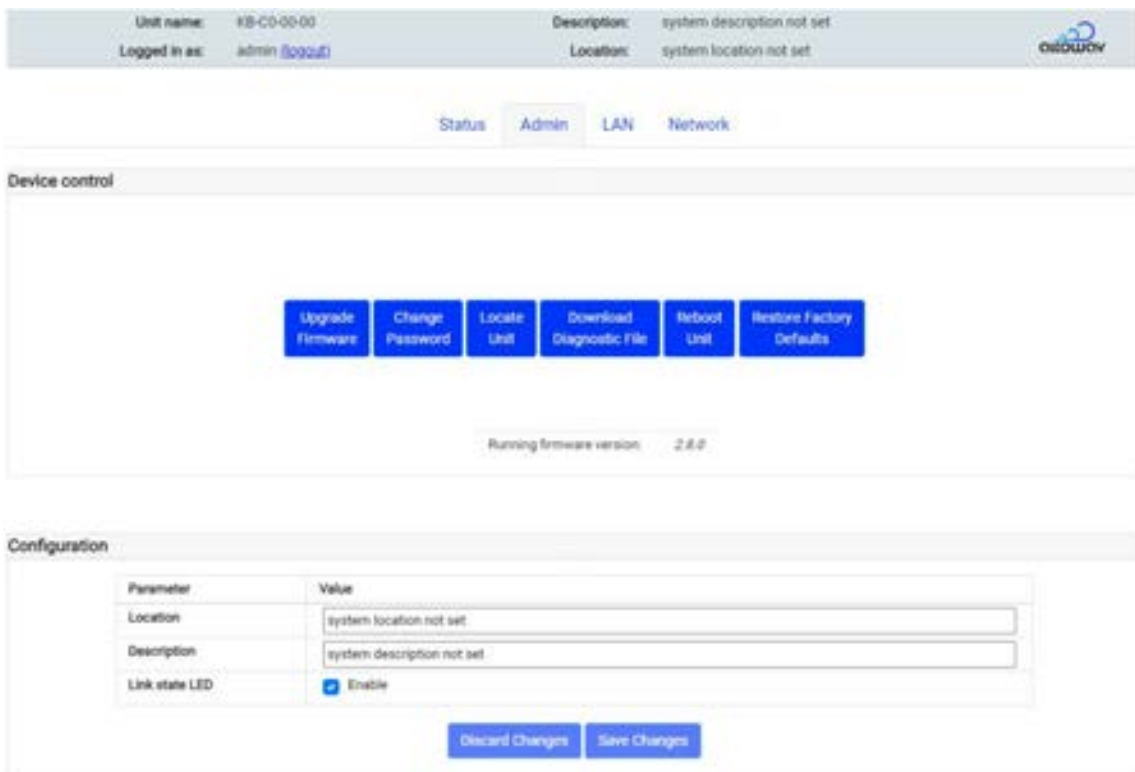
### Change a device password

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

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

To change the device password:

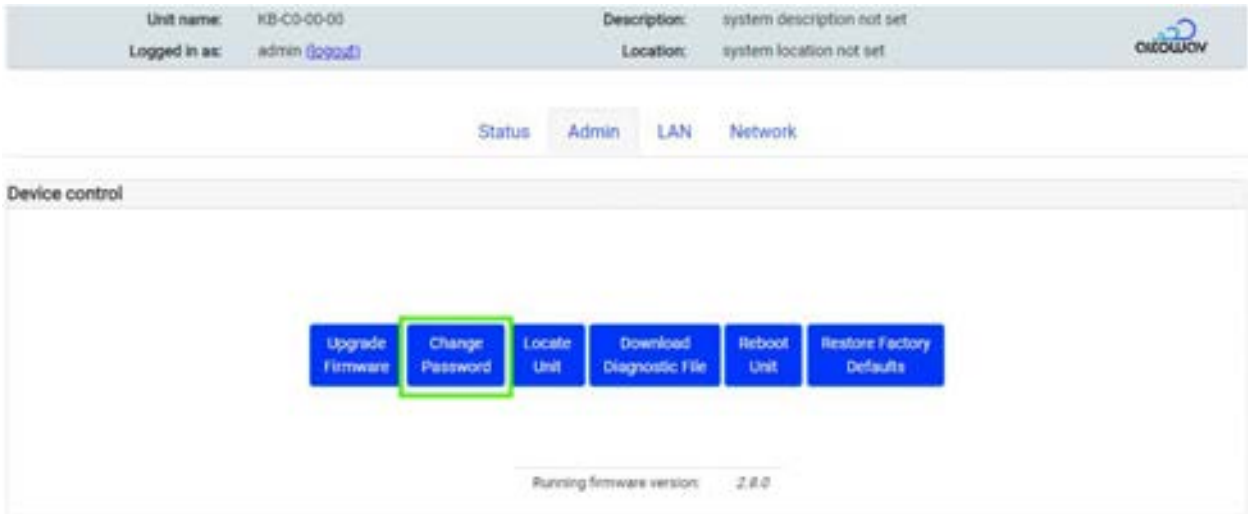
1. In the WebUI, click the **Admin** tab.



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



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



The **Change user password** dialog opens.

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



## Enable Passwordless SSH

By default, the C410 and 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 and C420.

1. Generate SSH keys on your local device.

2. log in via ssh to the C410 and C420:

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

where *hostname* is the hostname (for example. KB-C0-00-01) or IP address of the device.

3. Enter **control** mode:

```
KB-C0-00-01> control  
KB-C0-00-01(control)>
```

4. Use the **ssh\_keys** command:

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

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

## Upgrade firmware

### Upgrade roadmap

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

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

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

## Preliminary steps for using TFTP with the WebUI or CLI Method

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

1. Download and unzip the upgrade files from [Altoplex Firmware Downloads](https://support.altowav.com) at [support.altowav.com](https://support.altowav.com).

The following files are included in the zip file:

- A digest file
- The firmware file

The firmware filename consists of three parts:

`<product_name>-<device_family_name>-<version_number>`

where:

- *product\_name* is **kb\_sw-prod**
- *device\_family\_name* is one of:
  - **NOMAD** — Firmware used for D621 and P621 devices.
  - **DEVO** — Firmware used for C410, C420, and P421 devices.
- *version\_number* is the version number of the firmware.

For example:

kb\_sw-prod-DEVO-3.0.0

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

## Upgrade from the WebUI

### Upgrade from a local file

To upgrade from a local file by using the WebUI:

1. Download and unzip the upgrade files from [Altoplex Firmware Downloads](https://support.altowav.com) at [support.altowav.com](https://support.altowav.com).

The following files are included in the zip file:

- A digest file
- The firmware file

The firmware filename consists of three parts:

`<product_name>-<device_family_name>-<version_number>`

where:

- *product\_name* is **kb\_sw-prod**
- *device\_family\_name* is one of:
  - **NOMAD** — Firmware used for D621 and P621 devices.
  - **DEVO** — Firmware used for C410, C420, and P421 devices.
- *version\_number* is the version number of the firmware.

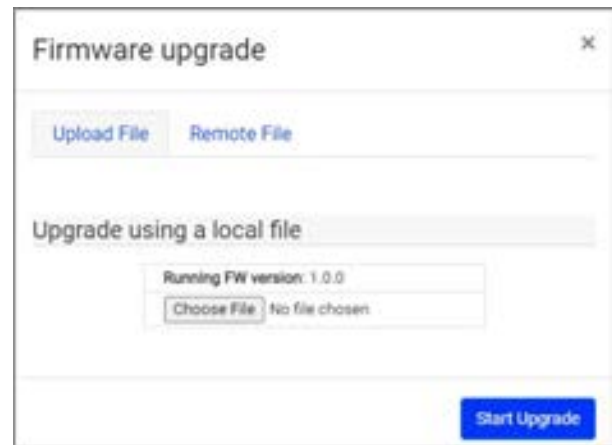
For example:

kb\_sw-prod-DEVO-3.0.0

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



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



## Upgrade from a TFTP server

1. Download and unzip the upgrade files from [Altoplex Firmware Downloads](http://support.altowav.com) at [support.altowav.com](http://support.altowav.com).

The following files are included in the zip file:

- A digest file
- The firmware file

The firmware filename consists of three parts:

`<product_name>-<device_family_name>-<version_number>`

where:

- *product\_name* is **kb\_sw-prod**
- *device\_family\_name* is one of:
  - **NOMAD** — Firmware used for D621 and P621 devices.
  - **DEVO** — Firmware used for C410, C420, and P421 devices.
- *version\_number* is the version number of the firmware.

For example:

kb\_sw-prod-DEVO-3.0.0

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



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

5. Click the **Remote File** tab.
6. For **TFTP server**, type the URL of the TFTP server.
7. Click **Check for Newer Firmware**.  
A message will indicate if the firmware on the TFTP server is newer than the firmware on the device.
8. If newer firmware is found, click **Start Upgrade**.



## Upgrade from the CLI

1. log in via ssh to the C410 and C420:  

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

where *hostname* is the hostname (for example. KB-C0-00-01) or IP address of the device.
2. Enter **control** mode:  

```
KB-C0-00-01> control
KB-C0-00-01(control)>
```
3. Query the TFTP server to determine if firmware on the server is newer than firmware on the device:  

```
KB-C0-00-01(control)> software check server_ip <IPv4-address-of-TFTP-server>
KB-C0-00-01(control)>
```
4. If newer firmware is available, a message will be displayed:  

```
update available: 3.0.0, image file: <firmware_filename>
```

The firmware filename consists of three parts:

`<product_name>-<device_family_name>-<version_number>`

where:

- *product\_name* is **kb\_sw-prod**
- *device\_family\_name* is one of:
  - **NOMAD** — Firmware used for D621 and P621 devices.
  - **DEVO** — Firmware used for C410, C420, and P421 devices.
- *version\_number* is the version number of the firmware.

For example:

kb\_sw-prod-DEVO-3.0.0

6. Upgrade the software:  

```
software upgrade server_ip <IPv4-address-of-TFTP-server>
```

After the software upgrade completes, the device will reboot.

## Upgrade from the REST API

1. Download and unzip the upgrade files from [Altoplex Firmware Downloads](https://support.altowav.com) at [support.altowav.com](https://support.altowav.com).

The following files are included in the zip file:

- A digest file
- The firmware file

The firmware filename consists of three parts:

`<product_name>-<device_family_name>-<version_number>`

where:

- *product\_name* is **kb\_sw-prod**
- *device\_family\_name* is one of:
  - **NOMAD** — Firmware used for D621 and P621 devices.
  - **DEVO** — Firmware used for C410, C420, and P421 devices.
- *version\_number* is the version number of the firmware.

For example:

kb\_sw-prod-DEVO-3.0.0

2. Upload the firmware image file to a server that can be access by all devices.
3. Use the `configuration/software_upgrade` API to install the firmware file. For example:
 

```
curl -k -X POST -u admin:<password> -H "Content-Type:application/octet-stream" -H "X-File-Name:<path>/<filename>" --data-binary @<path>/<filename> https://<hostname>/rest/v002/configuration/software_upgrade
```

Where:

- *password* is the password to log into the device. The default password is **admin**.
- *path* is the path to the firmware file. If the command is executed from the same local directory as the firmware file, path is not necessary.
- *filename* is the name of the firmware upgrade file, for example, kb\_sw-prod-DEVO-3.0.0.
- *hostname* is the hostname or IP address of the device being upgraded.

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

```
$ curl -i -k -X POST -u admin:admin \
-H "Content-Type:application/octet-stream" \
-H "X-File-Name:kb_sw-prod-DEVO-3.0.0.plain" \
--data-binary @kb_sw-prod-DEVO-3.0.0.plain \
https://10.0.0.01/rest/v002/configuration/software_upgrade
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 34.1M 100 88 100 34.1M 15 6358k 0:00:05 0:00:05 --:--:-- 6301kHTTP/1.1
100 Continue
HTTP/1.1 200 OK
Content-Type: application/json
```

```
Cache-Control: public, must-revalidate, proxy-revalidate
Content-Length: 88
Date: Sat, 01 Jan 2022 00:23:39 GMT
Server: lighttpd/1.4.73
{
  "status": "starting",
  "running-sw-version": "2.9.0",
  "upgrade-running": "yes"
}
```

The upgrade may take up to several minutes to complete.

## Verify that the firmware update was successful

### Verify firmware update from the command line

1. log in via ssh to the C410 and C420:

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

where *hostname* is the hostname (for example. KB-C0-00-01) or IP address of the device.

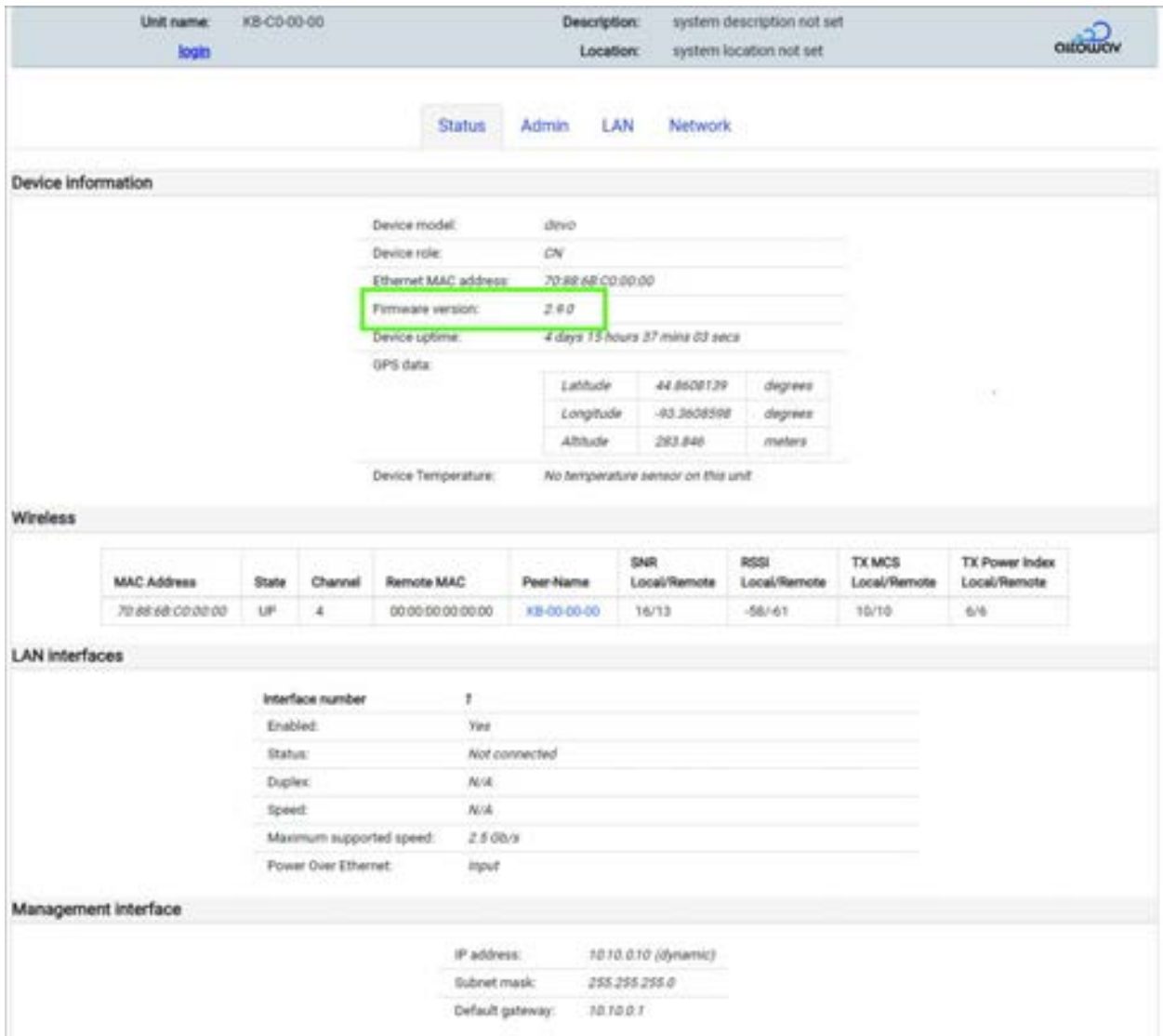
2. Check the status of the device by using the **kb\_device\_status** command:

```
KB-C0-00-01> kb_device_status
[Device: KB-C0-00-01, HW name: devo, software: 3.0.0]
description: test iteration 32
location: system location not set
authorized_org:
led_enable: enable
date: Thu Oct 25 14:32:24 UTC 2024
uptime: 14:32:24 up 3 days, 16:07, 1 users, load average: 1.10, 1.11, 1.09
DNS Servers: 10.80.0.252
Radio Link:
Radio Local MAC          Local Intf  Remote MAC          Status CN
-----
wlan0 00:00:00:00:00:00  terra0     00:00:00:00:00:01  UP      KB-C0-00-02
KB-C0-00-01>
```

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

## Verify firmware update from the WebUI

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



The screenshot shows the WebUI interface for a device. At the top, there is a header with the unit name 'XB-C0-00-00', a description 'system description not set', and a location 'system location not set'. Below this is a navigation bar with tabs for 'Status', 'Admin', '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 '2.0.0'. Other device information includes the device model 'd8vo', device role 'CN', Ethernet MAC address '70:88:68:C0:00:00', and device uptime of '4 days 13 hours 37 mins 03 secs'. GPS data is also displayed, including latitude, longitude, and altitude. The 'Wireless' section shows a table with one entry for the wireless interface. The 'LAN interfaces' section shows details for interface '1', which is enabled but not connected. The 'Management interface' section shows the IP address '10.10.0.10 (dynamic)', subnet mask '255.255.255.0', and default gateway '10.10.0.1'.

Unit name: XB-C0-00-00  
Description: system description not set  
Location: system location not set

login

Status Admin LAN Network

Device information

Device model: d8vo  
Device role: CN  
Ethernet MAC address: 70-88-68-C0-00-00  
Firmware version: 2.0.0  
Device uptime: 4 days 13 hours 37 mins 03 secs

GPS data:

Latitude	44.8608129	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
70-88-68-C0-00-00	UP	4	00-00-00-00-00-00	XB-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

Management interface

IP address: 10.10.0.10 (dynamic)  
Subnet mask: 255.255.255.0  
Default gateway: 10.10.0.1



## 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-C0-00-01kb-c0-00-e6/rest/v002/device/
node_identity
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100   605    100   605     0     0    8188     0  --:--:--  --:--:--  --:--:--  8402{
  "Ethernet MAC" : "70:88:6B:C0:00:00",
  "HW name" : "devo",
  "HW rev" : 2,
  "HW type code" : 82,
  "Node role" : "CN",
  "Number Ethernet Interfaces" : 1,
  "Number RF Interfaces" : 1,
  "Part number" : "1900-8411-1012-devo-2-LBKA0ZZ1SV1",
  "Serial number" : "0000000000000000000000001KB-C0-00-00:2",
  "authorized_org" : "",
  "bootloader version" :
"KBBLVERSION:1.3:prod:robot:2024-10-25_11-57-10:devo:1b565eb",
  "description" : "system description not set",
  "gps available" : 1,
  "location" : "system location not set",
  "name" : "KB-C0-00-01",
  "node type" : "PTP",
  "software" : "3.0.0"
}
```

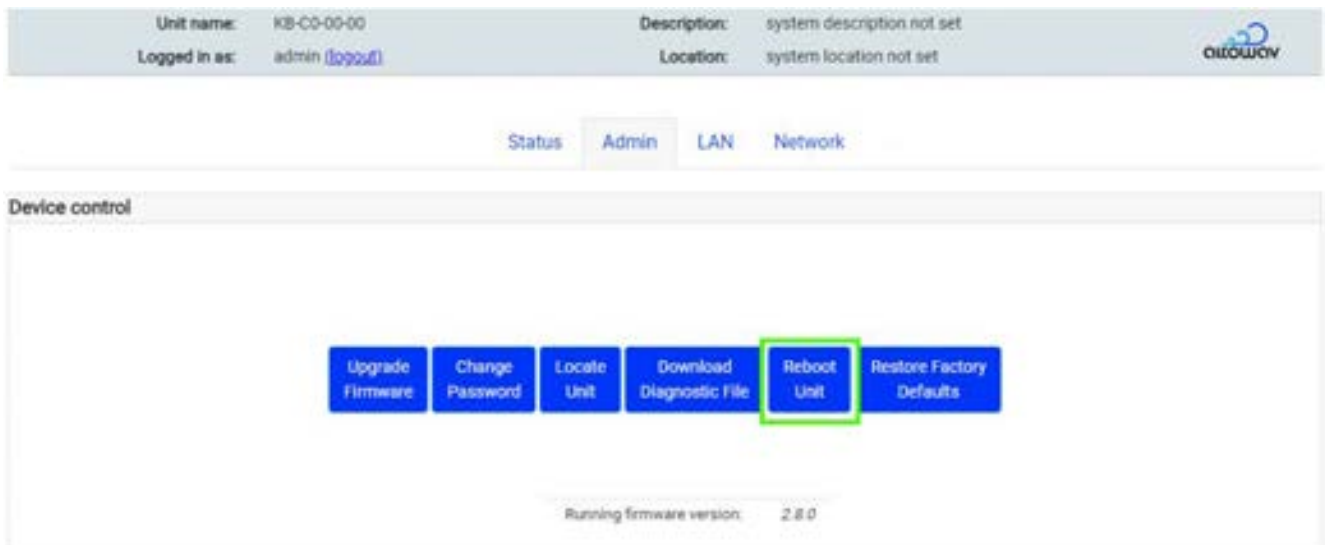
## Reboot

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

1. C410/C420 devices default to DHCP for IP assignment. Access the WebUI by browsing to the hostname or IP address. For example, if your network has a DHCP server and hostname resolution, type **https://<hostname>/** in the browser's address bar to access the WebUI for the device.
2. Click the **login** link in the WebUI header to log in as administrator. The username is **admin**, and the default password is **admin**.



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



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

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

## Factory Reset

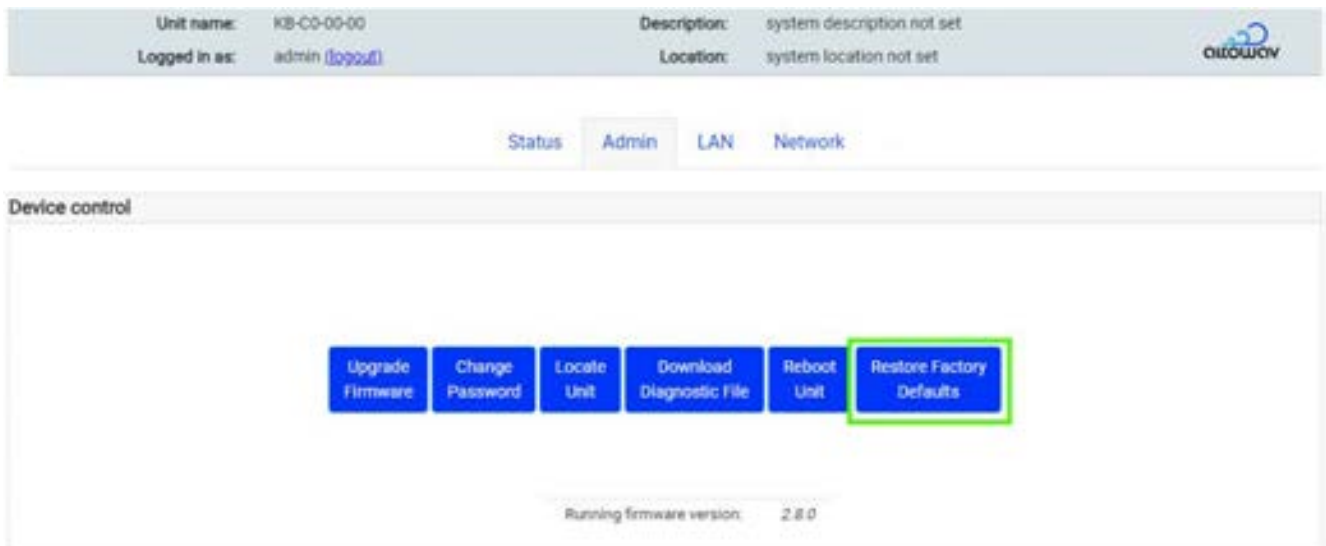
### Restore factory defaults by using the WebUI

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

1. C410/C420 devices default to DHCP for IP assignment. Access the WebUI by browsing to the hostname or IP address. For example, if your network has a DHCP server and hostname resolution, type **https://<hostname>/** in the browser's address bar to access the WebUI for the device.
2. Click the **login** link in the WebUI header to log in as administrator. The username is **admin**, and the default password is **admin**.



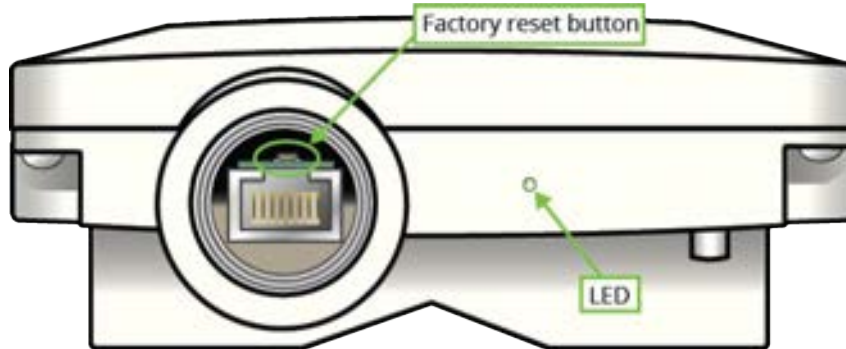
3. Click on the **Admin** tab, entering the password to log in when prompted.
4. Click on the **Restore Factory Defaults** button in the **Device control** section and wait until the reboot is complete.



## Restore factory defaults by using the factory reset button

If the WebUI is inaccessible due to a lost password or in cases where network settings are inadvertently set to unworkable values, use the following hard factory reset steps. After the reset, normal operation resumes with factory default settings.

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

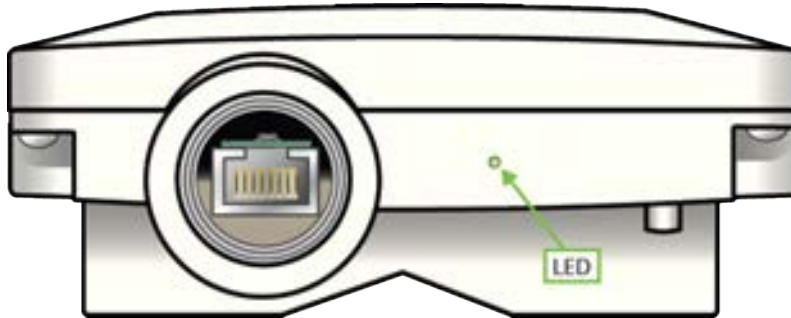
## Troubleshooting

This chapter contains the following topics:






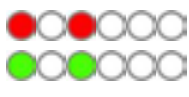
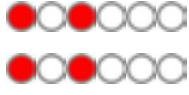
- [LED Indicators](#)
- [Lost Password](#)
- [How to Run a Diagnostic Dump](#)

## 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 <a href="#">Factory Reset</a> 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 <a href="#">factory reset</a> .
	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

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](mailto: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.

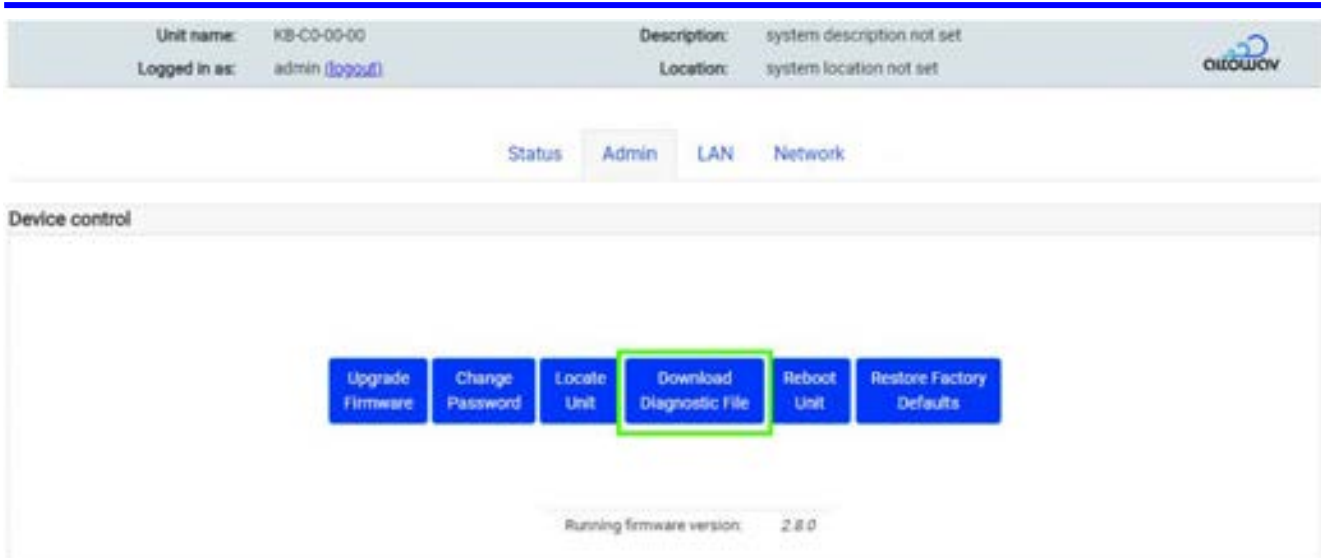
**Note:** A diagnostic log file captures historical information about a device's operation. It is important to download the diagnostic file before rebooting or power-cycling a device as part of troubleshooting. Rebooting or power-cycling will clear the log file history.

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

1. C410/C420 devices default to DHCP for IP assignment. Access the WebUI by browsing to the hostname or IP address. For example, if your network has a DHCP server and hostname resolution, type **https://<hostname>/** in the browser's address bar to access the WebUI for the device.
2. Click the **login** link in the WebUI header to log in as administrator. The username is **admin**, and the default password is **admin**.



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



1. The file is sent to your system's default download location. The file name includes the host name (KB MAC) of the device and the date. For example, KB-C0-00-01\_diag\_2024-10-25-20-32-26.txt
2. Zip the file and attach it to an email to [support@altowav.com](mailto:support@altowav.com) or a ticket at [support.altowav.com](https://support.altowav.com).

## Create a diagnostic file from the REST API

1. Use the `admin/diagdump` API to create a diagnostic file from the REST API. For example, use the `curl` command to save the diagnostic information to a file named `diag_dump`, created in the current directory:  
`curl -k -o diag_file.txt -u admin:<password> https://<hostname>/rest/v002/admin/diagdump`  
*where:*
  - *password* is the password to log into the device. The default password is **admin**.
  - *hostname* is the hostname or IP address of the device.
2. Zip the file and attach it to an email to [support@altowav.com](mailto:support@altowav.com) or the ticket at [support.altowav.com](https://support.altowav.com).



# 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-C0-00-01.

**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 [client nodes](#).

**DN** — See [distribution node](#).

**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 [distribution node](#) 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.

