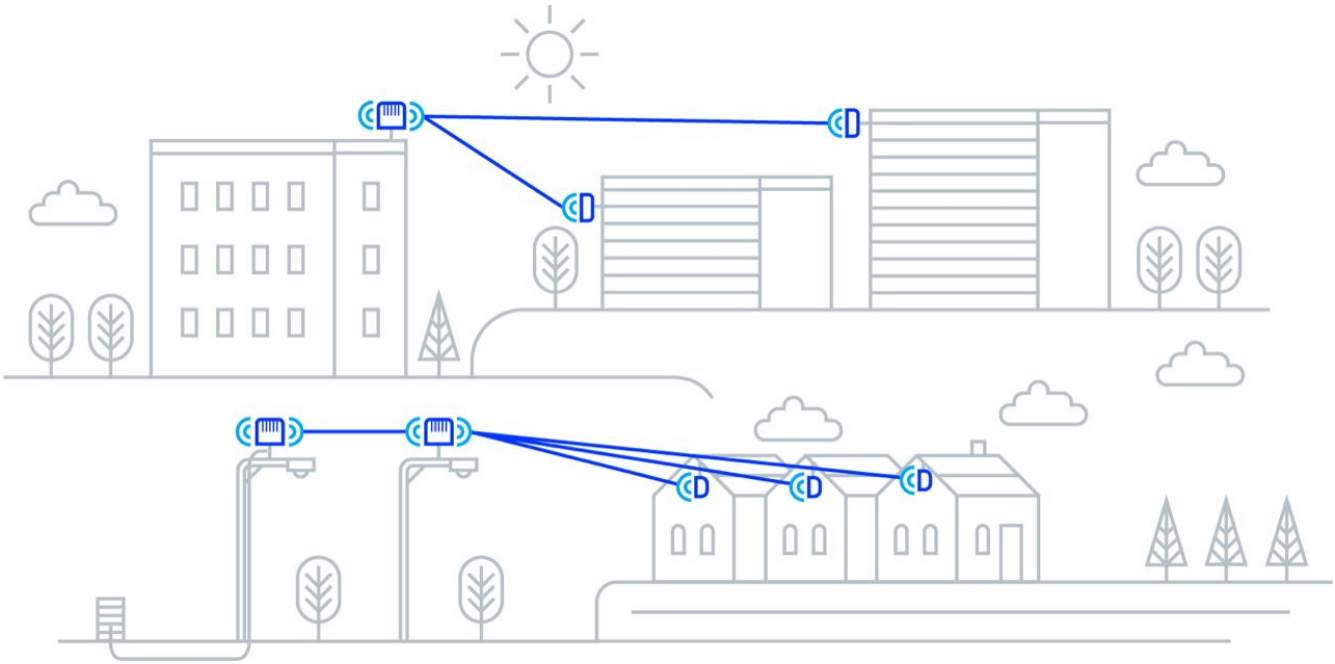


AltoCommand User Guide

December 31, 2024

Copyright, trademark, and legal information

For full Regulatory notices and statements, refer to the manufacturer and product as declared on the hardware label.

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

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

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

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

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

Revision history

Revisions	Date
Rebranded product to AltoCommand. Includes: • Support for all Altowav devices. • Authenticated communication between AltoCommand and AltoPlex devices. • Threshold configuration for incident reports. • Rebeamform settings.	12/31/2024
Initial release of the Edge Manager User Guide.	6/27/2024

Contents

AltoCommand User Guide Overview

Thank you for choosing the Altowav AltoCommand management software for advanced access to your Altowav network. This user guide describes the installation of AltoCommand, initial network setup, common management tasks, and provides a reference of its features and functions.

This guide is intended for network administrators or technicians who will monitor and optimize network performance, as well as perform network management tasks, such as adding / removing devices, upgrading device software, and managing users.

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 and organization of the network they are managing.

Related documentation

Further information about installing Altowav's 60 GHz network devices can be found at https://support.altowav.com/.

Additional help

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

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

AltoCommand Introduction

Altowav's AltoCommand offers advanced access to your network. AltoCommand is designed to provide functions for Altowav's AltoPlex networks and devices that off-the-shelf tools cannot deliver.

In keeping with Altowav's goal to *Elevate Your Network*, the AltoCommand is designed to monitor earlier Altowav devices: the K60, K60c, K60c+, K60i, and K60x. AltoCommand has read-only access to earlier Altowav devices.

AltoCommand makes site administration easier in the following ways:

- The **Dashboard** quickly brings network issues to the attention of the site administrator.
  - Devices down.
  - Incidents of poor RSSI, poor MCS, links flapping, and links down.
  - Show firmware version compliance and number of devices per type.
  - Device registration status, to allow authenticated communication with AltoCommand (AltoPlex devices only).
- Investigate issues and areas for optimization
  - View incidents by role during a specific time period, and see their current status.
  - View and compare graphs of different metrics for a specific Incident, time, link or device.
  - Visualize links, channels, and device positions via the Map.
  - Analyze long-term quality and investigate with **Analytics**.
- Simplify common administrative tasks, such as:
  - Investigating details and generating log data for specific links or devices.
  - Link quality reporting.
  - Device configuration.
  - Device upgrades.
  - Network setup and device discovery.
  - Configure incident thresholds and rebeamforming activities (AltoPlex devices only).
  - Managing users / permissions.

AltoCommand installation

This topic describes how to install AltoCommand as supplied by Altowav — on a fanless industrial PC with software loaded. Installing the AltoCommand hardware and setting up a new network relies on having operational Altowav DNs (for example, the D621 or P621) or Hubs (for example, the K60) in place per the working network design.

Prerequisites

- An outbound connection to the internet is required to use the Map and to download software updates.
- Network access:
  - The Ethernet port labeled **LAN 1** on the AltoCommand device is set to DHCP by default. To remotely access the device, the installer/administrator needs access the DHCP-assigned IP address. Look for a DHCP server lease with a MAC address beginning with **00:e2:69** to identify the IP address assigned to the AltoCommand.
  - The Ethernet port labeled **LAN 4** on the AltoCommand device has a default IP address and netmask of 192.168.100.1/24. To use this port, your laptop or PC will need to be configured to use an IP address in the 192.168.100.x network.

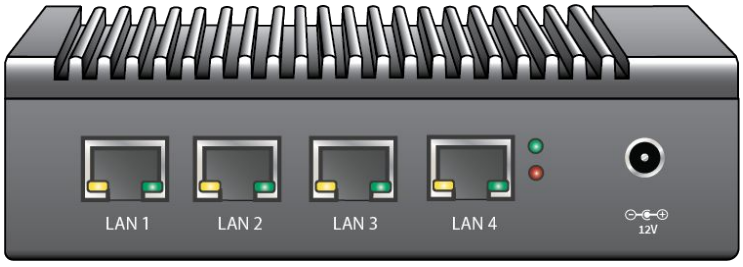
Install the AltoCommand hardware at the network site

These steps describe how to install the AltoCommand as supplied by Altowav, power it up and log in.

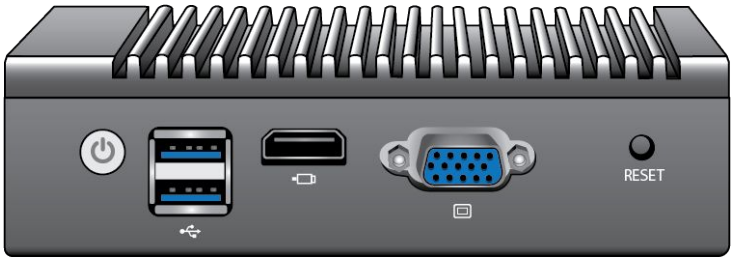
1. **Connect the AltoCommand hardware.** Connect LAN port 1 to a network-connected switch or similar, or LAN port 4 to a PC configured to use the 192.168.100.x network.

   See Prerequisites for more information about the LAN ports on the the AltoCommand hardware.

2. **Power up.** Plug the supplied power cord into the 12V port and into a standard outlet.



   The LEDs will light up, indicating the power is on. If they do not light, push the power button on the back of the device.



3. **Browse to the AltoCommand hardware's IP address**.
4. This brings up a login dialog. (If you receive a browser warning that the site is not secure, click the **Advanced** button and click the **Proceed to...** link.)

   Default credentials for login:

   User Name: **admin**

   Password: **admin**

   AltoCommand management software opens on the **Settings** page for the initial setup. See Set up a new network for steps to name the network, add devices and adjust them on the **Map** for optimal use.

Set up a new network

After Installing the AltoCommand, complete the initial network setup by naming the site and adding the IP address(es) of distribution nodes (DNs) or Hub devices. Doing this populates your network site with the DNs or Hub devices as well as any CNs or Remotes to which they are connected.

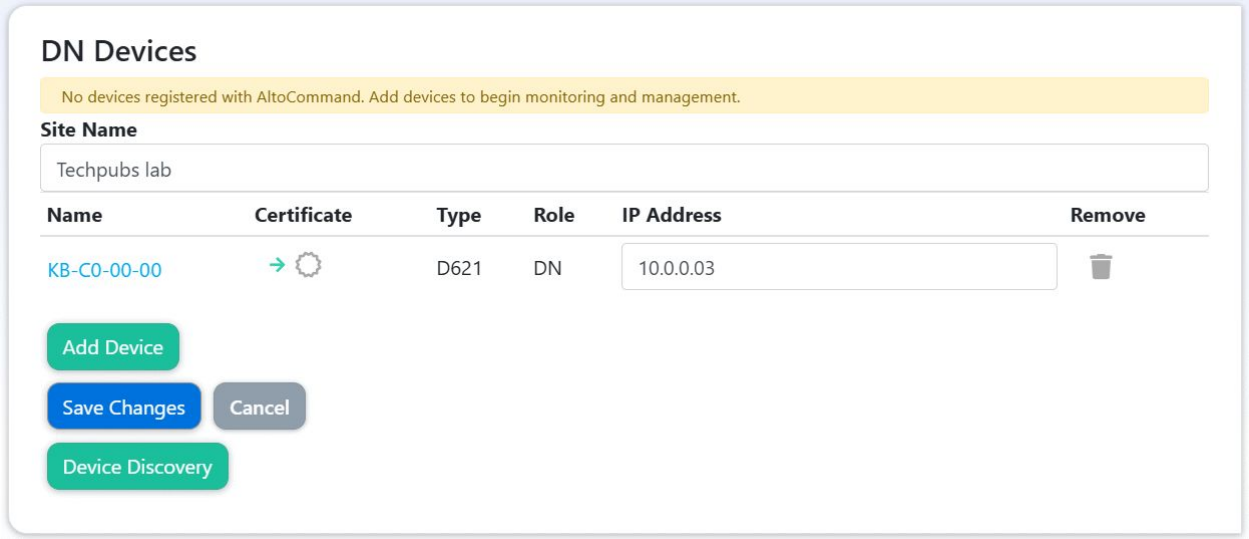
For new installations, until you configure a site name and add a device, AltoCommand will automatically open to the **Site Devices** tab on the **Settings** page.

Instructions for specific devices follow.

Initial network site setup for AltoPlex DNs

1. Enter the network **Site Name**.
2. Click **Add Device**.
3. Enter the **IP Address** of an installed and connected DN.

   Note: By default, AltoPlex devices use DHCP to acquire an IP address. If the IP address of the DN changes, the AltoCommand will no longer recognize the device. Therefore, when using AltoPlex devices with AltoCommand, best practice is to configure your DHCP server to use IP reservation for DNs, or to assign static IP addresses to DNs.



> **Tip:** Enter the DN at the point of presence (PoP) node for the most efficient device discovery.

4. Click **Device Discovery**. All connected devices are discovered and populate the list.
   - If the list is complete, **Save Changes**.
   - If the list is not complete, check that all site devices are connected and operating. Adjust as needed and when all expected devices are active, run **Discovery** again.

Or, if you prefer to add devices manually, click **Add Device** and enter the IP addresses manually.

5. Instruct AltoCommand to install a certificate (AltoPlex devices only).

   The SSL client certificate allows the AltoCommand software to have SSL-based authentication to AltoPlex devices, which provides write access to the device without requiring the device's password.

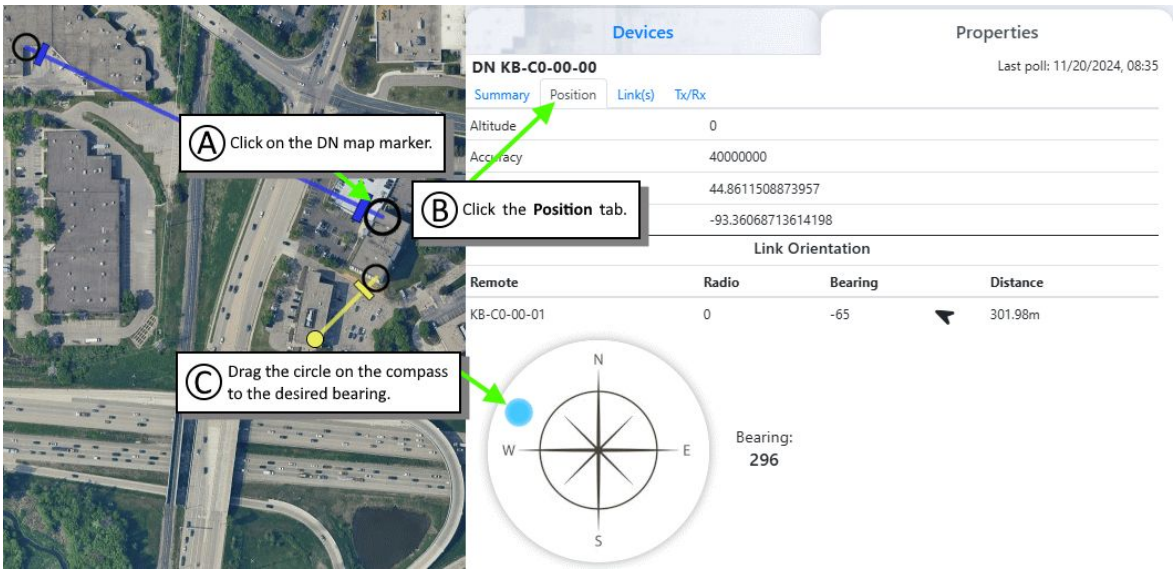
   A. In the **Certificate** column, click the icon next to a new device.

      AltoCommand will install a certificate on the device. When the certificate installation is complete, the icon will change to .

   B. Repeat for each device.

   See Device authentication for more information.

6. After all devices are added, go to the Map and adjust the bearing for the DNs. This improves the accuracy of the Map for the purposes of planning, monitoring and optimizing the network.
   A. Click the map marker for the DN.
   B. Click **Position**.
   C. Drag the circle on the compass to the desired bearing.

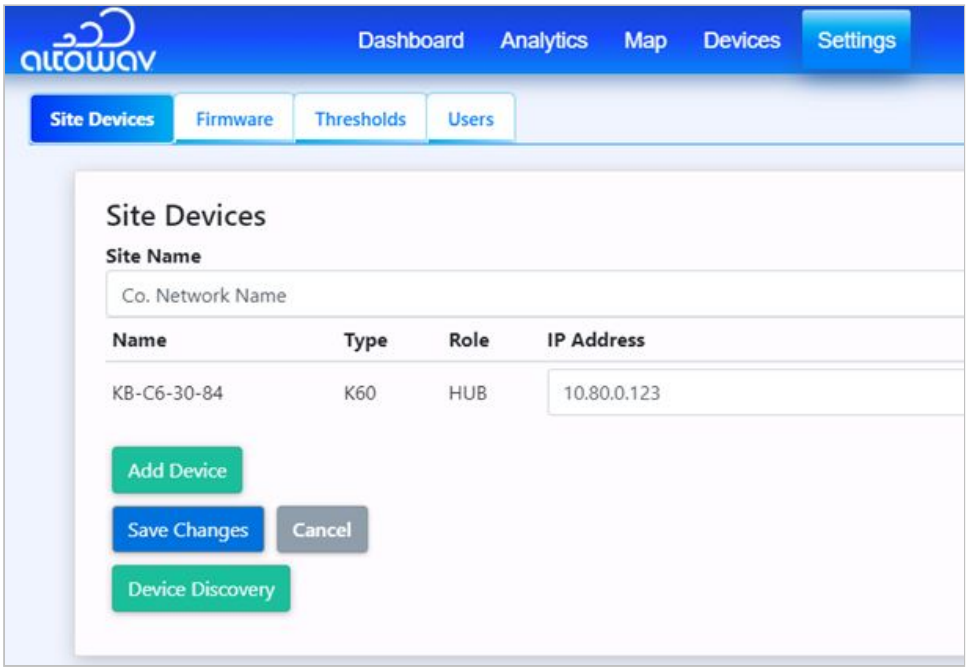


7. Any connected CN devices are automatically populated to the Map. Adjust a CN's map position by simply dragging to its actual installation location. This improves the accuracy of the Map for the purposes of planning, monitoring and optimizing the network.

Initial network site setup for K60 or K60c Hubs

1. Enter the network **Site Name**.
2. Click **Add Device**.
3. Enter the **IP Address** of all installed Hub devices (typically K60s). The Hubs should be configured for connection, installed and powered up to be added to the network. Then, click **Save Changes**.

   Note: By default, K60 and K60c Hubs use DHCP to acquire an IP address. If the IP address of the Hub changes, the AltoCommand will no longer recognize the device. Therefore, when using K60 and K60c Hubs with AltoCommand, best practice is to configure your DHCP server to use IP reservation for Hubs, or to assign static IP addresses to Hubs.



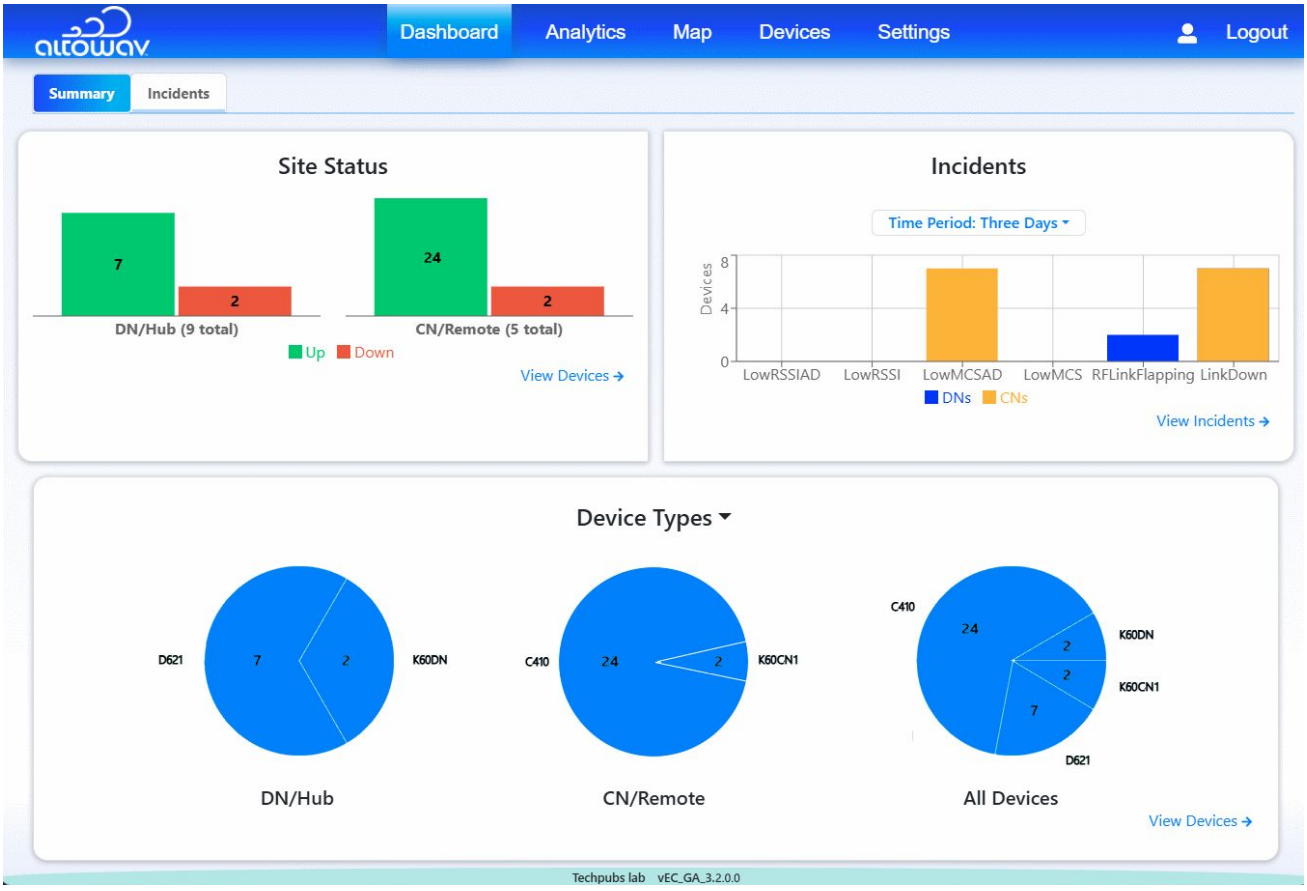
4. Go to the Map and drag the Hub device markers from the tray to the desired map location.
5. **Adjust the bearing** for each Hub.
   A. Click the map marker for the Hub.
   B. Click on **Position** in the sidebar.
   C. Drag the circle on the compass to the desired bearing.
6. Any connected Remote devices are automatically populated to the Map. Adjust a Remote's map position by simply dragging to its actual installation location. This improves the accuracy of the Map for the purposes of planning, monitoring and optimizing the network.

Monitoring and optimizing tasks

AltoCommand is designed to alert the site administrator to potential problems. The following monitoring and optimizing tasks are described through samples.

- Quickly see devices that are down.
- Investigate incident reports, including:
  - How to configure incident reporting.
  - How to investigate reported incidents of links down, when all devices are up.
  - How to configure wireless connections to rebeamform automatically.
- Review a network on a map.
- Use AltoCommand to refine network performance.
- Find and update devices with out-of-date software.

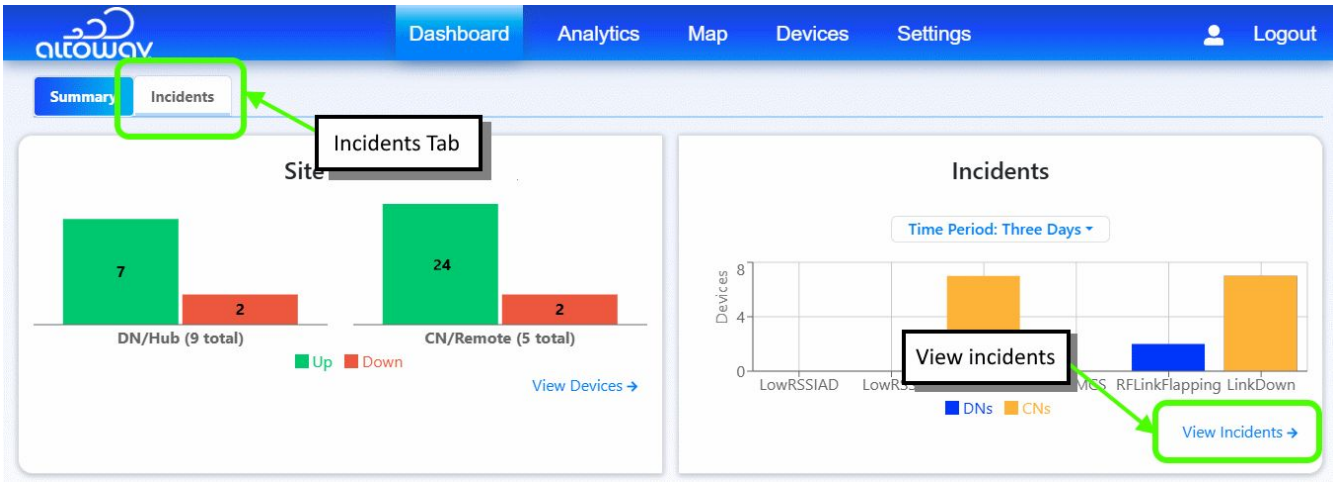
The **Dashboard** provides a quick assessment of network health.



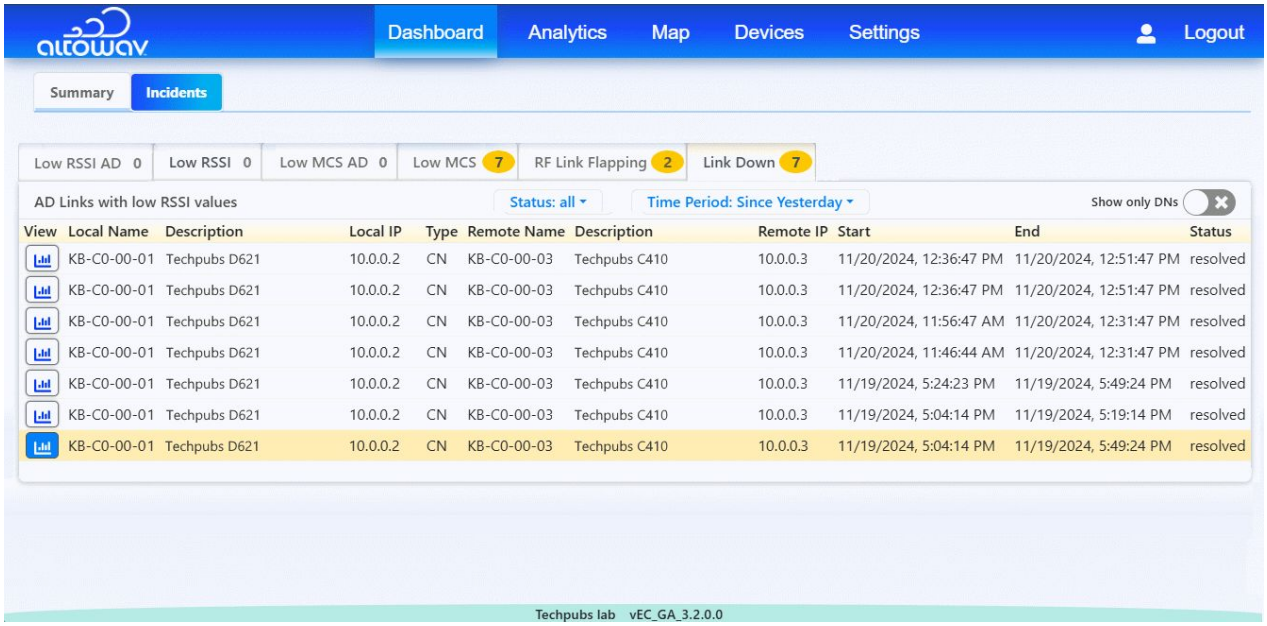
Task: Investigate incident reports

The **Incident** pane of the the AltoCommand **Dashboard Summary** tab provides a visual display of any reports of problems with your Altowav network.

To investigate reported incidents, click **View Incidents →** or click the **Incidents** tab.



The **Incidents** tab is displayed:



Tabs provide access to information about specific categories of incidents:

Low RSSI — Lists reported incidents when the average RSSI value is less than the configured threshold. Two tabs are available:

- **Low RSSI AD** — Applies to earlier (802.11ad) versions of Altowav products.
- **Low RSSI** — Applies to AltoPlex (802.11ay) products.

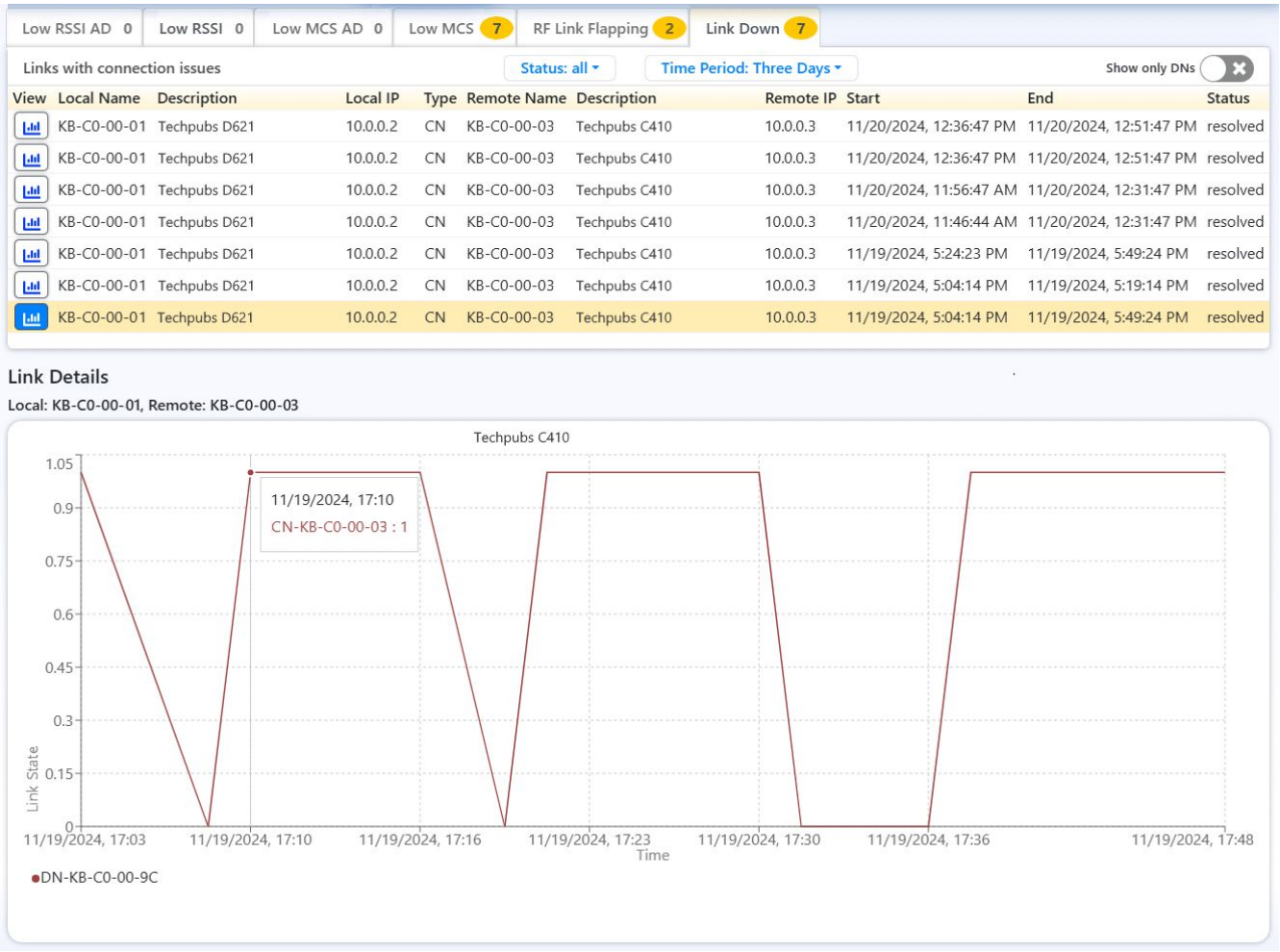
Low MCS — Lists reported incidents when the average weighted MCS level is less than the selected thresholds. Two tabs are available:

- **Low MCS AD** — Applies to earlier (802.11ad) versions of Altowav products.
- **Low MCS** — Applies to AltoPlex (802.11ay) products.

RF Link Flapping - The RF link goes down and comes back up more than the configured threshold.

Link Down - Link is reported as down.

Drill into specific details about an incident by clinking the **Graph** icon (📊) next to the incident to display a graph providing further details.



For further information about viewing incidents, see **Incidents** tab and Tips for viewing graphs.

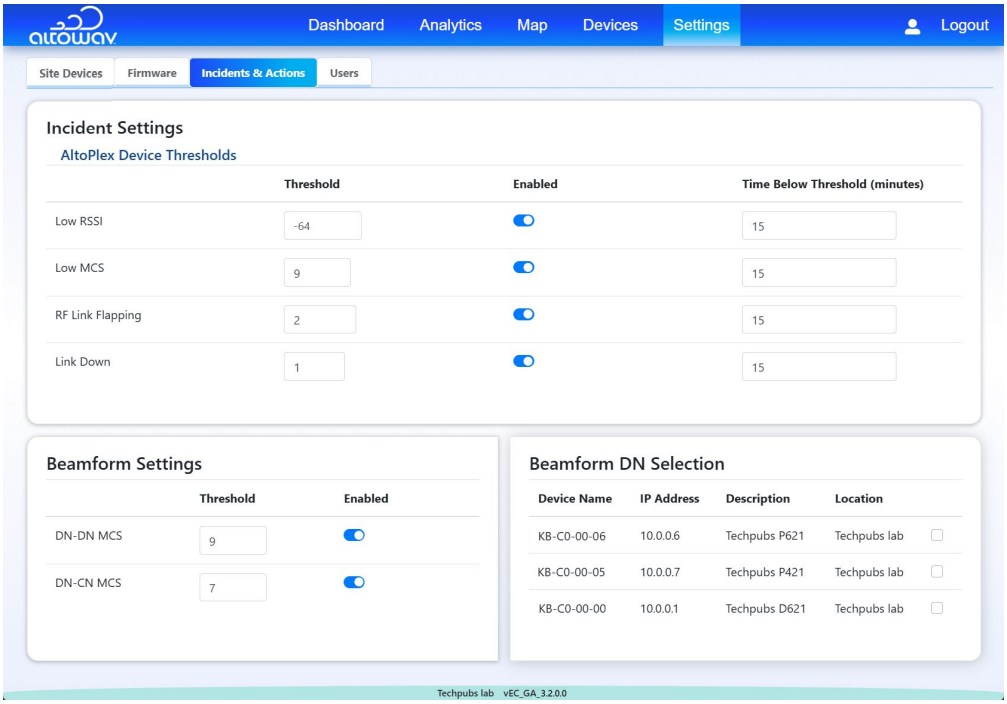
Configure incident reporting

Normally, default settings for incident reporting are sufficient. However, you can configure incident reporting thresholds and related settings on the **Settings** page.

Note: Incident threshold settings are only available for AltoPlex devices. This feature is not available for K60, K60c, K60c+, K60i, and K60x devices.

1. Click **Settings**.
2. Click **Incidents & Actions**.

The **Incidents & Actions** page displays.



The **Incidents Settings** pane is used to configure incident reporting by enabling/disabling incidents, as well as setting thresholds and intervals. The following incidents are available for configuration:

Low RSSI — RSSI (Received Signal Strength Indicator) is a measurement of how well a device can receive signals from external wireless devices. The higher the number, the better the signal strength. By default, when the average RSSI for a device is below -64 dBm for 15 minutes, an incident report is logged and displayed on the **Incidents** tab of the **Dashboard**.

Low MCS — MCS (Modulation Coding Scheme) is a measurement of how efficiently data is being transferred over a wireless connection. AltoPlex devices use a weighted MCS value of 2-12. By default, when the average weighted MCS of a device is below 9 for 15 minutes, an incident report is logged and displayed on the **Incidents** tab of the **Dashboard**.

RF Link Flapping — Link flapping refers to a link that goes down and comes back up. By default, if a device has two link flapping incidents in a period of 15 minutes, an incident report is logged and displayed on the **Incidents** tab of the **Dashboard**.

Link Down — By default, if a link is reported as down for 15 minutes, an incident report is logged and displayed on the **Incidents** tab of the **Dashboard**.

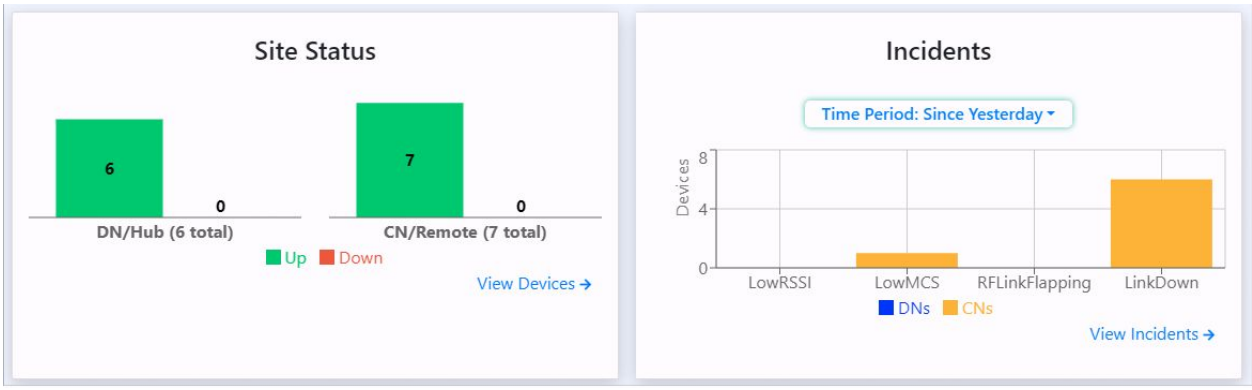
3. For each incident setting, set the appropriate threshold, enable/disable the incident report, and set the time.

Example: Investigate reports of links being down, when all devices are up

In the sample shown, no links are down, but several incidents of LinkDown have been reported. If the issue is ongoing, this could be caused by physical obstructions to the line of sight (LOS), such as tree branches, movement of the device due to mounting issues, etc.

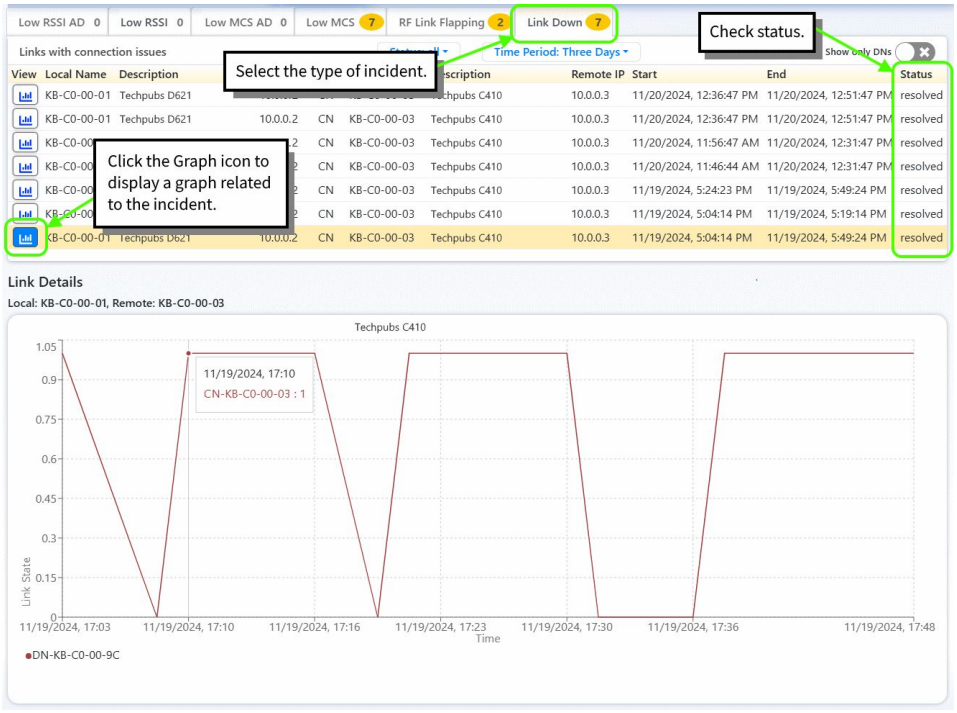
The following steps show one method of investigating the issue. Steps will vary per specific network environment.

1. View the **Dashboard**.



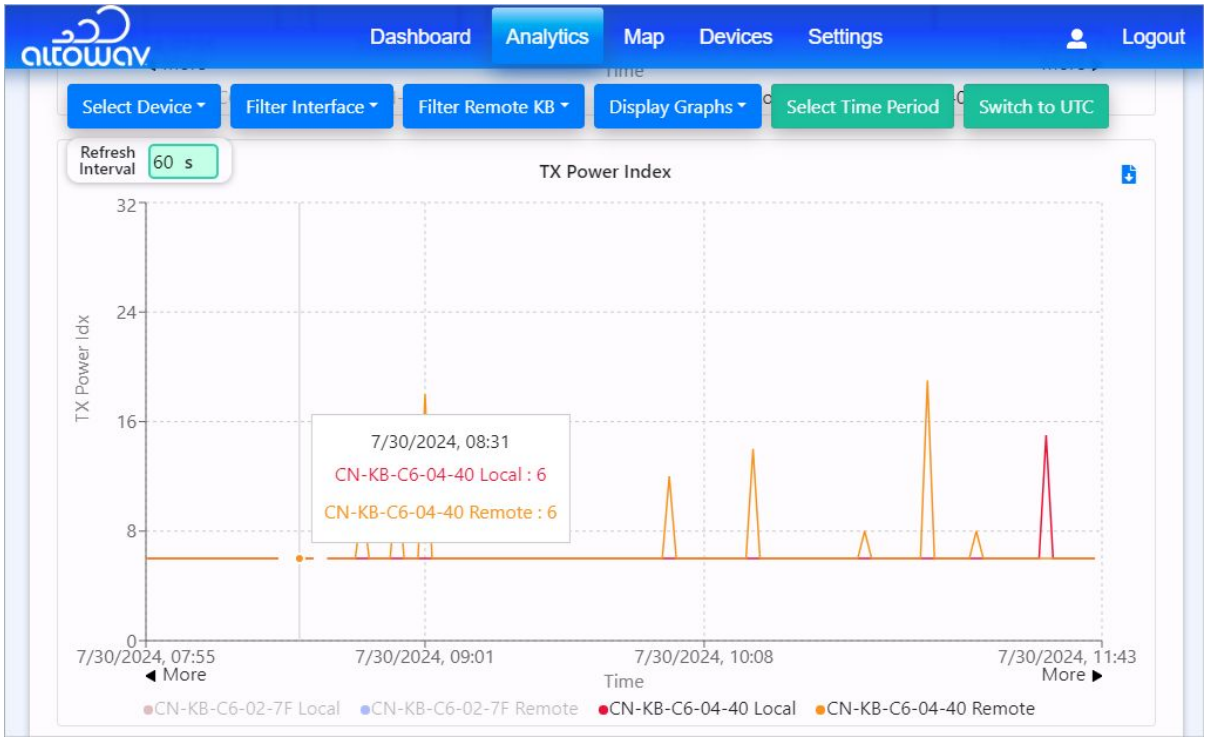
   - **Site Status** indicates that all links are currently up.
   - **Incidents** indicates that there were several links down in the last day.
2. Click **View Incidents →**.
3. Click on the **Link Down** tab to view a list of Link Down incidents.

   Review the **Status** column to see if the issues are resolved, recurring or new. Click on the **Graph** icon (📊) to to display related graphs for any incident.



4. Hover at problematic areas on the graph such as a break or dip in the line, to determine the time of an incident.

5. Click **Analytics** and scroll through the analytics graphs to view correlating data, such as power index and throughput, for the time of the incident. In this case, a break in the TX Power Index is shown for that device, during the time of the incident.


Dashboard
Analytics
Map
Devices
Settings
Logout
Select Device
Filter Interface
Filter Remote KB
Display Graphs
Select Time Period
Switch to UTC
Refresh Interval
60 s
TX Power Index
TX Power Idx
32
24
16
8
0
7/30/2024, 08:31
CN-KB-C6-04-40 Local : 6
CN-KB-C6-04-40 Remote : 6
7/30/2024, 07:55
7/30/2024, 09:01
7/30/2024, 10:08
7/30/2024, 11:43
◀ More
Time
More ▶
CN-KB-C6-02-7F Local
CN-KB-C6-02-7F Remote
CN-KB-C6-04-40 Local
CN-KB-C6-04-40 Remote

Task: Configure automated rebeamforming

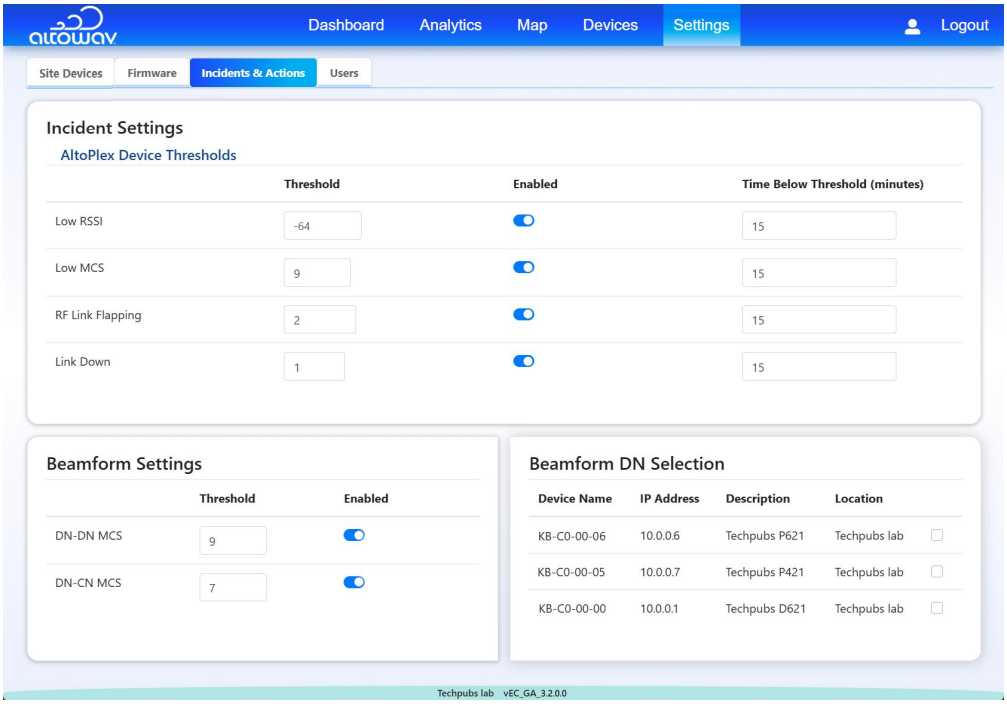
Rebeamforming is a process by which a wireless connection between two devices is taken down, and a new connection is formed. The default behavior for Altowav devices is to periodically reform beams every four hours, regardless of the quality of the beam.

With AltoCommand, you can disable periodic rebeamforming and use an automated rebeamforming mechanism instead. With automated rebeamforming, AltoCommand performs rebeamforming based on configured MCS threshold values.

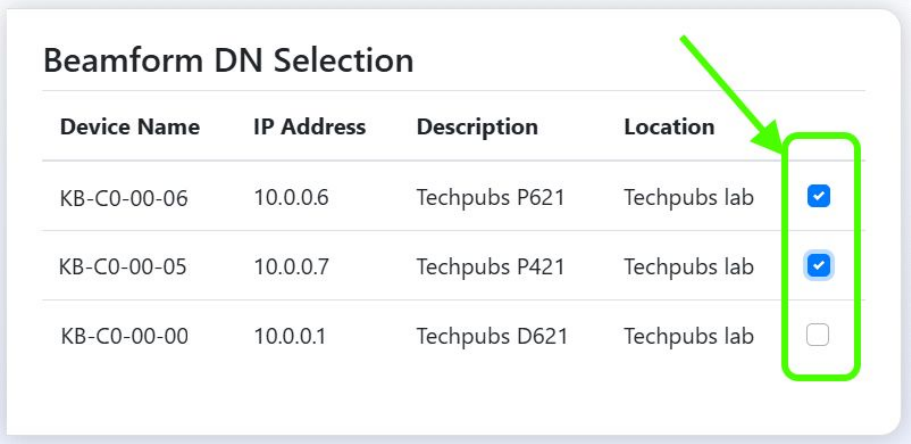
Note: Beamform threshold settings are only available for AltoPlex devices. This feature is not available for K60, K60c, K60c+, K60i, and K60x devices.

1. Click **Settings**.
2. Click **Incidents & Actions**.

   The **Incidents & Actions** page displays.

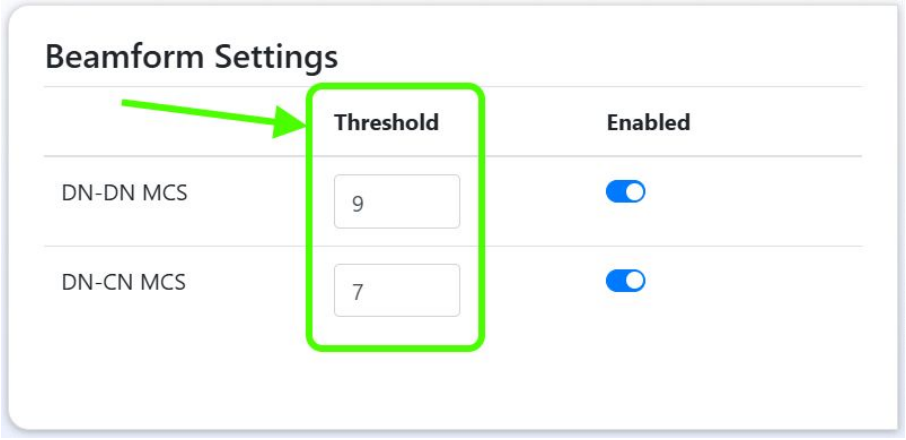


- If the configured MCS settings for DN and CN links are appropriate for your network, in the **Beamform DN Selection** pane, enable automated rebeamforming by clicking the checkbox at the end of the row for each applicable device.



- To configure MCS settings for DN and CN links:
  1. In the **Beamform Settings** pane, set the **Threshold** for both DN to DN and DN to CN links.

     The MCS threshold value represents the average weighted MCS, sampled every 60 seconds, over a period of one hour.



     - When a wireless connection is performing above the configured MCS threshold value, rebeamforming will not be performed.
     - When the connection falls below the configured threshold, rebeamforming will be performed automatically.
     - After a link is reformed, AltoCommand will wait two hours to rebeamform again, regardless of the quality of the link.
  2. To disable beamform settings for a particular type of link, toggle off **Enable** for either DN-DN or DN-CN links.

Troubleshooting rebeamforming issues

If a wireless connection is regularly being rebeamformed by the automated rebeamform feature, the line of sight between the two devices should be inspected to determine if there are any physical obstructions that may be causing the link to have poor performance. Alternatively, you can disable automated rebeamforming on devices with problematic links; however, this will reenable the device's periodic rebeamforming.

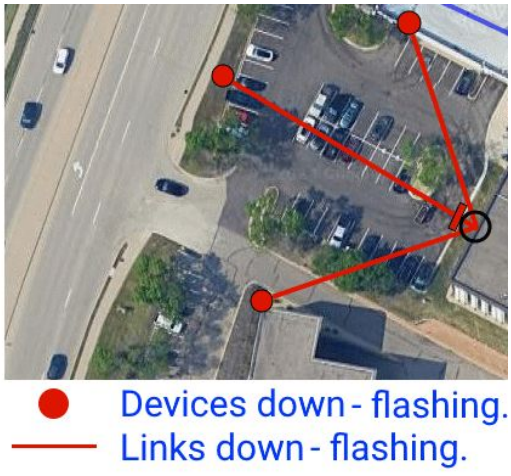
Task: Review a network using the Map

See Set Up a New Network for information about populating the Map with your network. After a new network is set up, and clients are being added to the network, ongoing review of the network via the Map is recommended.

However, for devices without GPS or with GPS disabled, this visual review requires that the positioning of the devices is accurate on the Map. Drag devices to reposition them.

Look at the Map for the following issues.

- Any flashing red links, indicating the links are down.
- Any flashing red device markers, indicating the devices are down.



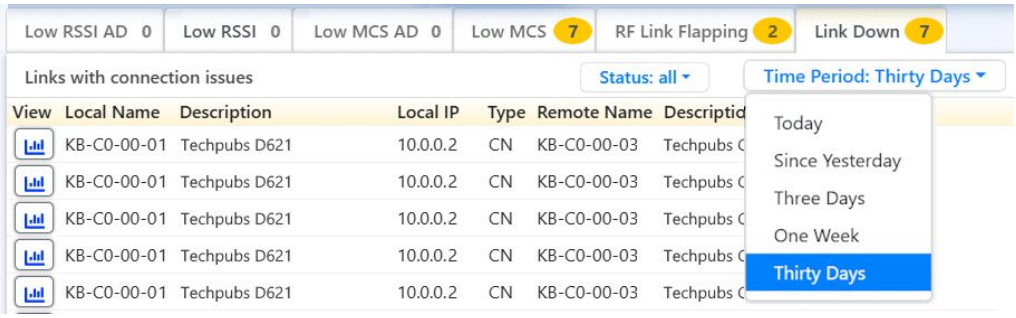
- Potential areas of interference due to butterfly, co-channel interference, or other configurations. This is most easily seen from the Map page, where the RF channels are shown by color, and relative distances and positions are easily visualized. For mitigation information, see the device's user guide.
- Potential area of improvement with beam elevation changes. For example when CNs are installed close to the connecting DN.
- Potential areas of poor performance due to link distances. This distance varies per device.

Task: Use AltoCommand to refine network performance

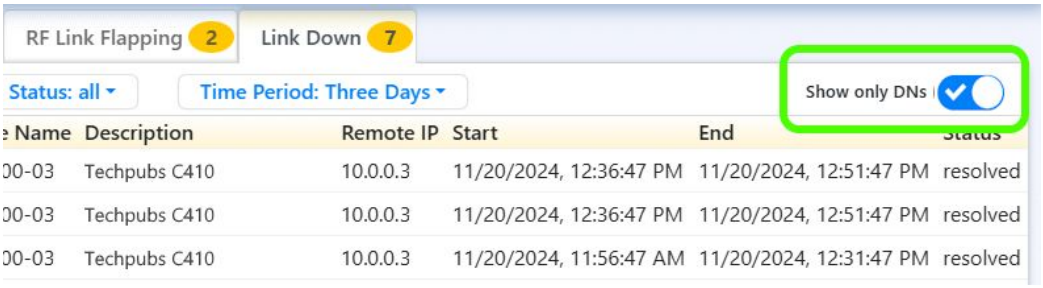
The overall performance of the network has been good. But best practices tell us to periodically review performance and make adjustments for improvement. Generally this means reviewing link performance for the following parameters, within a longer time period.

- Low average MCS
- Low RSSI issues
- High TX power
- High Packet error Rates
- Link flapping

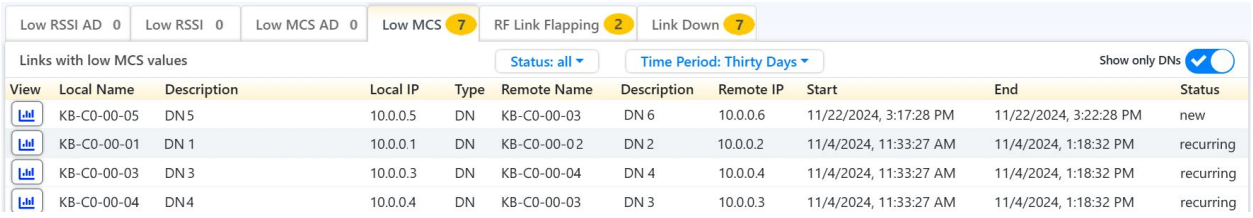
1. Go to the **Dashboard** and select the **Incidents** tab.
2. Set the time period to **One Week** or **Thirty Days**.



3. Enable **Show only DNs**.



4. Identify areas of concern where Incidents, such as low MCS or low RSSI, recur for the same device or link. For example, in this view of Low MCS incidents, we can see that the DN to DN link between DN1 and DN2 has recurring issues.
5.

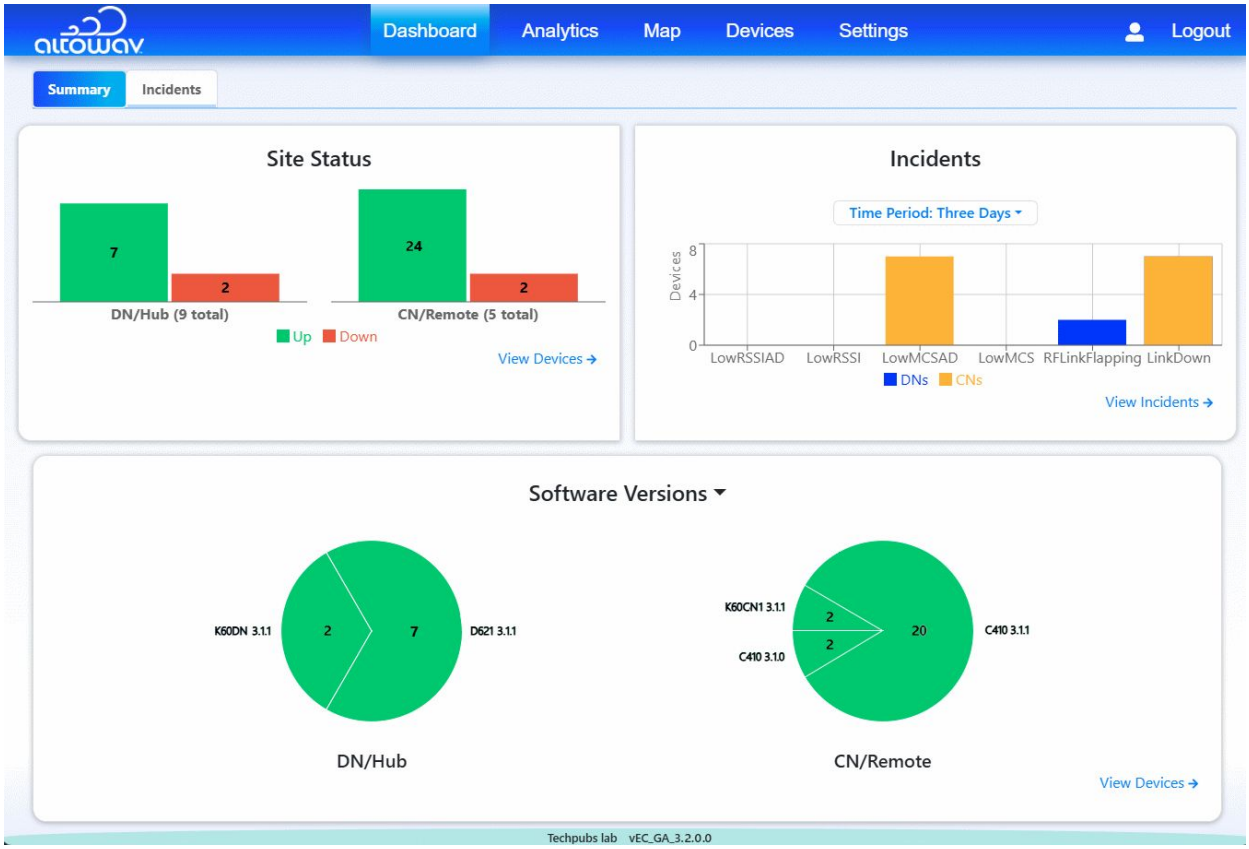


6. Use the Map to determine whether there are environmental factors that could be causing the issue. Check for interference due to:
   - Topology
   - Co-channel

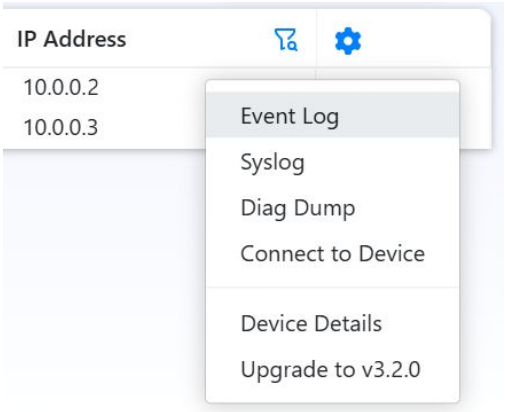
- Off boresight.

Task: Update software

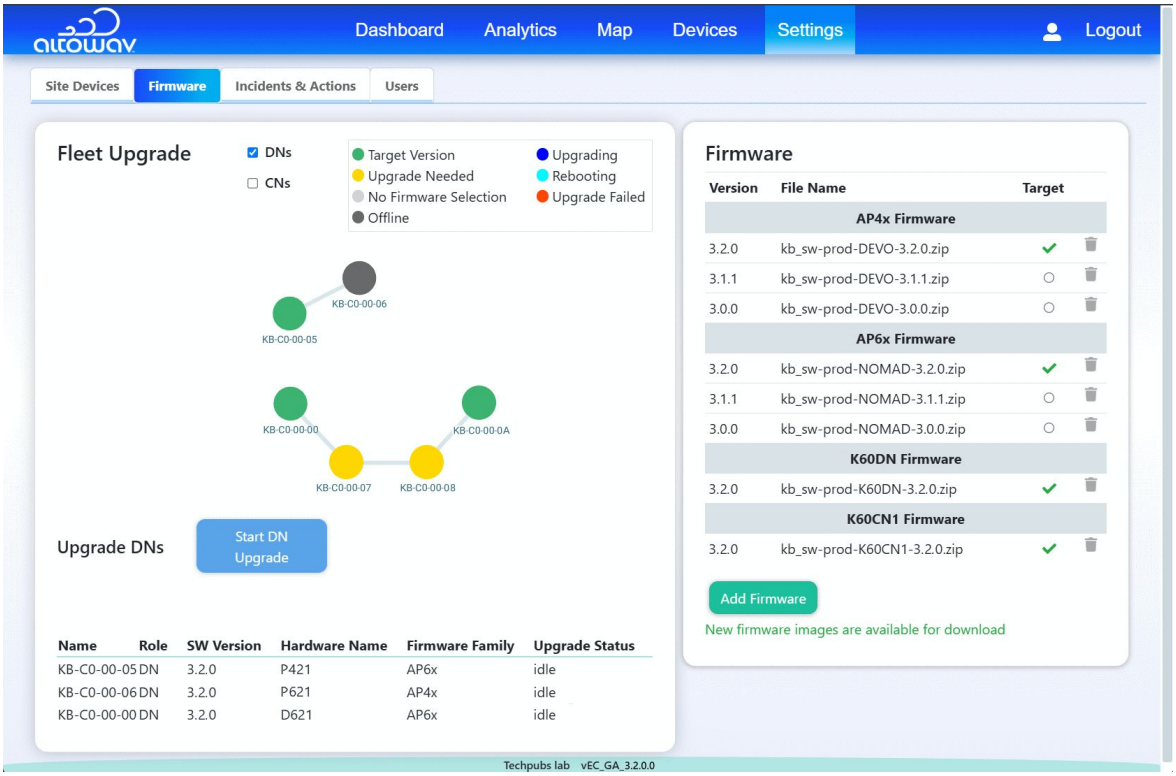
1. Go to the **Dashboard** to view the current **Software Versions** for all network devices.



2. Upgrade and manage device firmware with one of these methods:
   - Click on the **View Devices** link. Identify devices with outdated software versions. Click the ☰ menu in the **Settings** column and select the **Upgrade to...** option to upgrade a single device.



   - Click **Settings**, then click the **Firmware** tab and use the tools available there to upgrade devices.


Dashboard
Analytics
Map
Devices
Settings
Logout
Site Devices
Firmware
Incidents & Actions
Users
Fleet Upgrade
DNs
CNs
Target Version
Upgrading
Upgrade Needed
Rebooting
No Firmware Selection
Upgrade Failed
Offline
KB-C0-00-06
KB-C0-00-05
KB-C0-00-00
KB-C0-00-0A
KB-C0-00-07
KB-C0-00-08
Upgrade DNs
Start DN Upgrade
Name Role SW Version Hardware Name Firmware Family Upgrade Status
KB-C0-00-05 DN 3.2.0 P421 AP6x idle
KB-C0-00-06 DN 3.2.0 P621 AP4x idle
KB-C0-00-00 DN 3.2.0 D621 AP6x idle
Firmware
Version File Name Target
AP4x Firmware
3.2.0 kb_sw-prod-DEVO-3.2.0.zip
3.1.1 kb_sw-prod-DEVO-3.1.1.zip
3.0.0 kb_sw-prod-DEVO-3.0.0.zip
AP6x Firmware
3.2.0 kb_sw-prod-NOMAD-3.2.0.zip
3.1.1 kb_sw-prod-NOMAD-3.1.1.zip
3.0.0 kb_sw-prod-NOMAD-3.0.0.zip
K60DN Firmware
3.2.0 kb_sw-prod-K60DN-3.2.0.zip
K60CN1 Firmware
3.2.0 kb_sw-prod-K60CN1-3.2.0.zip
Add Firmware
New firmware images are available for download
Techpubs lab vEC_GA_3.2.0.0

Common administrative tasks

The AltoCommand is designed to efficiently handle common tasks, such as adding a device to the network. The following administrative tasks are described here:

- Add a DN or Hub to the Network.
- Add a CN or Remote to the Network.
- Change an AltoCommand User Password or Information.
- Assist an AltoCommand User with a Lost Password.

See also Monitoring and Optimizing Tasks.

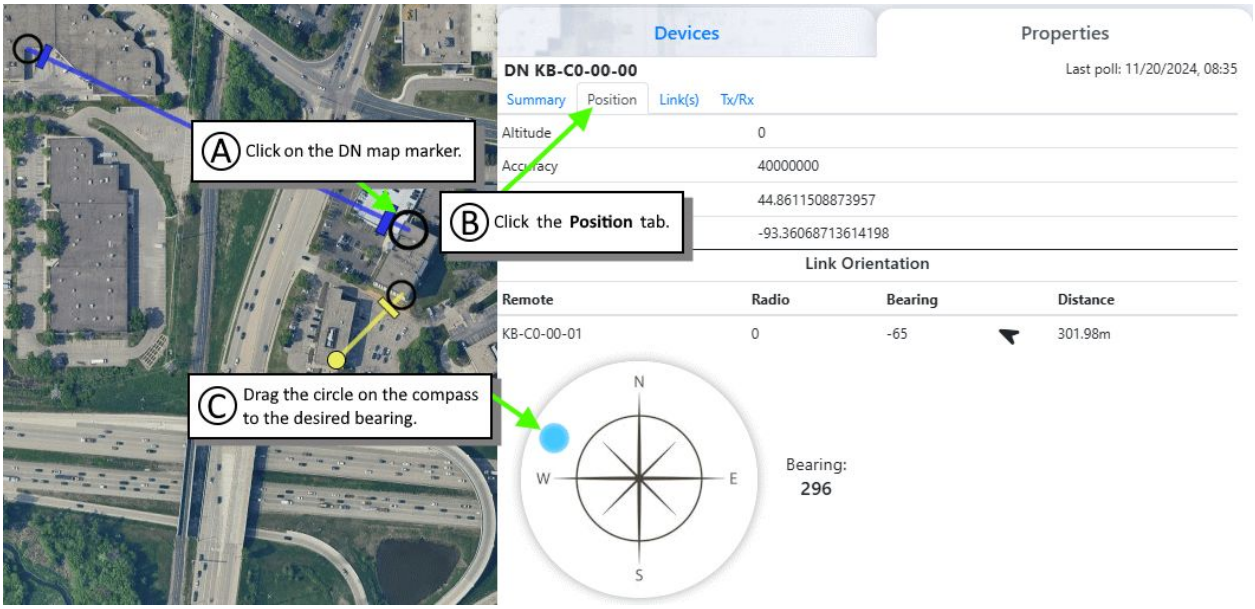
Add a DN or Hub to the network

Connecting a DN or Hub to an existing network automatically adds it to the AltoCommand network site. Typically, a device is connected during installation. See installation instructions for your specific device.

Note: AltoCommand regularly polls the network for newly added radios. However, when you add a radio, it may take a while for the polling to complete and for data to appear in AltoCommand.

New devices are listed on the **Dashboard**, **Analytics**, **Map**, **Devices** and **Settings** pages of the AltoCommand. For DNs with GPS enabled, a new marker will appear on the Map at the GPS location. For Hubs or DNs with GPS disabled, the marker is added to the device tray on the Map. In that case, the marker is positioned by dragging it to its actual installed location. Adjust the DN or Hub device bearing using the compass tool to match the device's actual azimuth:

1. Click the map marker for the DN.
2. Click **Position**.
3. Drag the circle on the compass to the desired bearing.



Note: Accurate positioning of the marker on the Map is important to communicate the correct information about device positions, RF Channel frequency and bearings.

Tips:
To position the new device marker at its installed location:

- Quickly find the new device marker in the Map. Hover over the new device's name in the Device list on the Map, and the map marker will grow. Or, hover over the map marker to highlight the Host Name in the Device list.
- Use the description, location and other network design information to drag the marker to the actual installed location on the Map in AltoCommand.

Steps for DNs and Hubs vary slightly, so examples are both shown.

DN Example: Add a new DN to an existing network.

1. Install the DN, ensuring a secure mounting, power and clear LOS to the active DN sector to which it will connect.
2. Configure the DN to form a wireless link to an existing DN:
    - For D621s, P421s, and P621s, use the DN link auto-configuration feature to automatically link the radios.
    - For K60DNs,
        - Enter the new DN's MAC address in the **DN Responder** field on the Wireless tab of the existing DN.
        - Enter the existing DN's MAC address in the **DN Responder** field on the Wireless tab of the new DN. Note, this is often completed during bench configuration before installation.
        - If the DN is a K60DN, be sure to add it to the correct Radio sector.

    See the device's documentation for detailed configuration and installation instructions.

3. Wait for the DNs to connect.
4. Go to the Map and adjust the new DN's bearing on the Map.

Optional ways to access the DN's WebUI for configuration.

- In the AltoCommand, click **Devices** in the top navigation bar and find the existing DN in the list. Click the **Menu** icon (☰) at the end of the row and select **Connect to Device**.
- On a network-connected PC, browse directly to the existing DN's IP address.

Hub Example: Add a new Hub to an existing network.

1. Configure the Hub to connect to the existing network.
2. Install the Hub, ensuring a secure mounting, power and clear LOS for any wireless links. Wait for the Hub to connect.
3. On the Map, drag the Hub from the device tray to its actual installed position.

See the device's documentation for detailed configuration and installation instructions.

Add a CN or Remote to the network

Connecting a CN or Remote to an existing network automatically adds it to the AltoCommand network. Typically, the device is connected during installation. See installation instructions for your specific CN or Remote device.

Note: AltoCommand regularly polls the network for newly added radios. However, when you add a radio, it may take a while for the polling to complete and for data to appear in AltoCommand.

New devices appear on the **Dashboard**, **Analytics**, **Map** and **Devices** list in the AltoCommand. On the Map, the new CN or Remote marker is added near its linked device. To improve Map accuracy, drag it to its actual installed location.

Note: Accurate positioning of the marker on the Map is important to communicate the correct information about device positions, RF Channel frequency, and bearings.

> **Tips:**
> To position the new device marker at its installed location:

> - **Quickly find the new device marker in the Map.** Hover over the new device's Name in the Device list on the Map, and the map marker will grow. This method works either way, that is, hovering over the map marker highlights the Device name in the list.

- **Use the Description**, **Location**, and other network design information to drag the marker to the actual installed location on the Map in AltoCommand.

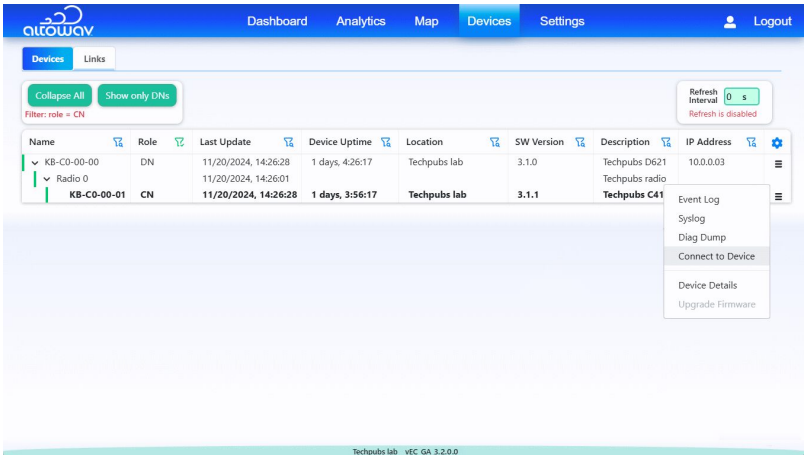
Steps vary slightly, so examples are shown for both CNs and Remotes.

CN Example: Add a new CN to an existing network.

1. Install the CN, ensuring a secure mounting, power and clear line of sight to the active DN to which it will connect.
2. Configure the link to the active DN by adding the CN's Host Name (KB-XX-XX-XX) to the DN's list of **CN Responders** and save the changes. Wait for the CN to connect. (If the DN is a K60DN, be sure to add it to the correct Radio sector.)
3. Adjust the CN's position on the Map.

Optional ways to access the CN's WebUI for configuration:

- In the AltoCommand:
    1. Click **Devices** in the top navigation bar.
    2. Click the Filter icon ().
    3. For the filter, select **Is equal to** and type **CN**.
    4. Find the CN in the list.
    5. Click the **Menu** icon () at the end of the row and select **Connect to Device**.
- On a network-connected PC, browse directly to the CN's IP address.



Remote Example: Add a new Remote to an existing network.

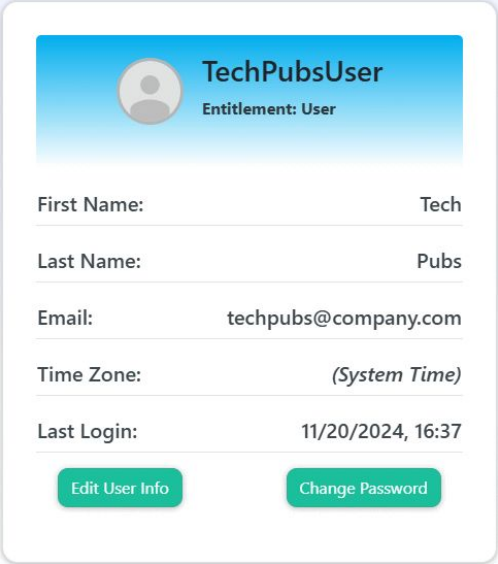
See the device's documentation for detailed configuration and installation instructions.

1. Configure the Remote to connect to the active Hub.
2. Install the Remote, ensuring a secure mounting, power and clear LOS to the active Hub. Wait for the Remote to connect.
3. Adjust the Remote's position on the Map.

Change user password or information

Each user has exclusive rights to change their information and password. However, a user with Admin privileges can add and delete users.

Click on the **User profile** icon ( ) in the top navigation bar to change user information or password.



Change Password requires you to confirm the password.

Lost password

Each user has exclusive access to their username and password. However, in the case of a lost password, an admin user can assist:

1. Navigate to Settings > Users.
2. Delete the user.
3. Add the user back with a new password.

Using earlier Altowav devices with AltoCommand

In keeping with Altowav's goal to *Elevate Your Network*, the AltoCommand is designed to monitor earlier Altowav devices: the K60, K60c, K60c+, K60i, and K60x. AltoCommand has read-only access to earlier Altowav devices.

Note: Altowav does not recommend blending earlier devices and AltoPlex devices at a single AltoCommand site.

Operational and terminology differences between earlier devices and AltoPlex arise mainly from the underlying technology standards.

- AltoPlex devices:
  - Are 802.11ay-based technology
  - Operate as **DN** (distribution nodes) or **CN** (client nodes).
- K60, K60c, K60c+, K60i, and K60x devices:
  - Follow 802.11ad standards
  - Are configured with **Hub** or **Remote** roles.
  - AltoCommand does not support **Remotes** on a link local network or a network that is not reachable by AltoCommand.

The following table outlines some differences that may clarify the terminology and operation of the devices in your network. Instructions in this guide use the terms shown below.

	AltoPlex		**K60, K60c, K60c+, K60i, and K60x**
Role	Distribution node (DN)	Client node (CN)	Hub, Remote
Models	• D621 (can be configured in either role) • P421 • P621 • K60DN	• D621 • C410 • C420 • K60CN1	• K60 • K60c
Number of sectors per device	**Typical:** 1-sector devices. **Exception:** K60DN may have up to 4 sectors.	1	1
Settings > Device Discovery	**Device Discovery** button auto discovers connected DNs and populates **Site Devices** list.		N/A
Initial Map Positioning	DNs with GPS available and enabled are auto positioned on the **Map**.	CNs with GPS available and enabled are auto	No GPS available.

		positioned on the **Map**. CNs without GPS are added to the **Map**, near their connected DN.	**Hubs** require manual positioning on the Map. **Remotes** are added to the Map, near their connected Hub.

AltoCommand Reference

Use this reference to look up the functions and operations available on each page of the AltoCommand.

Dashboard -- Use the dashboard **Summary** for a current overall view of the site status, incidents over a selected time period and current firmware versions. The **Incidents** tab of the dashboard shows more detail about incidents, the devices affected, current incident status, and shows graph data related to the incidents.

Analytics -- Provides the controls you need to look at device operation over a specified time. Select the performance metrics, time period, devices, and filter by interface to view the data you need. View analytics in graphical form or as Raw Data.

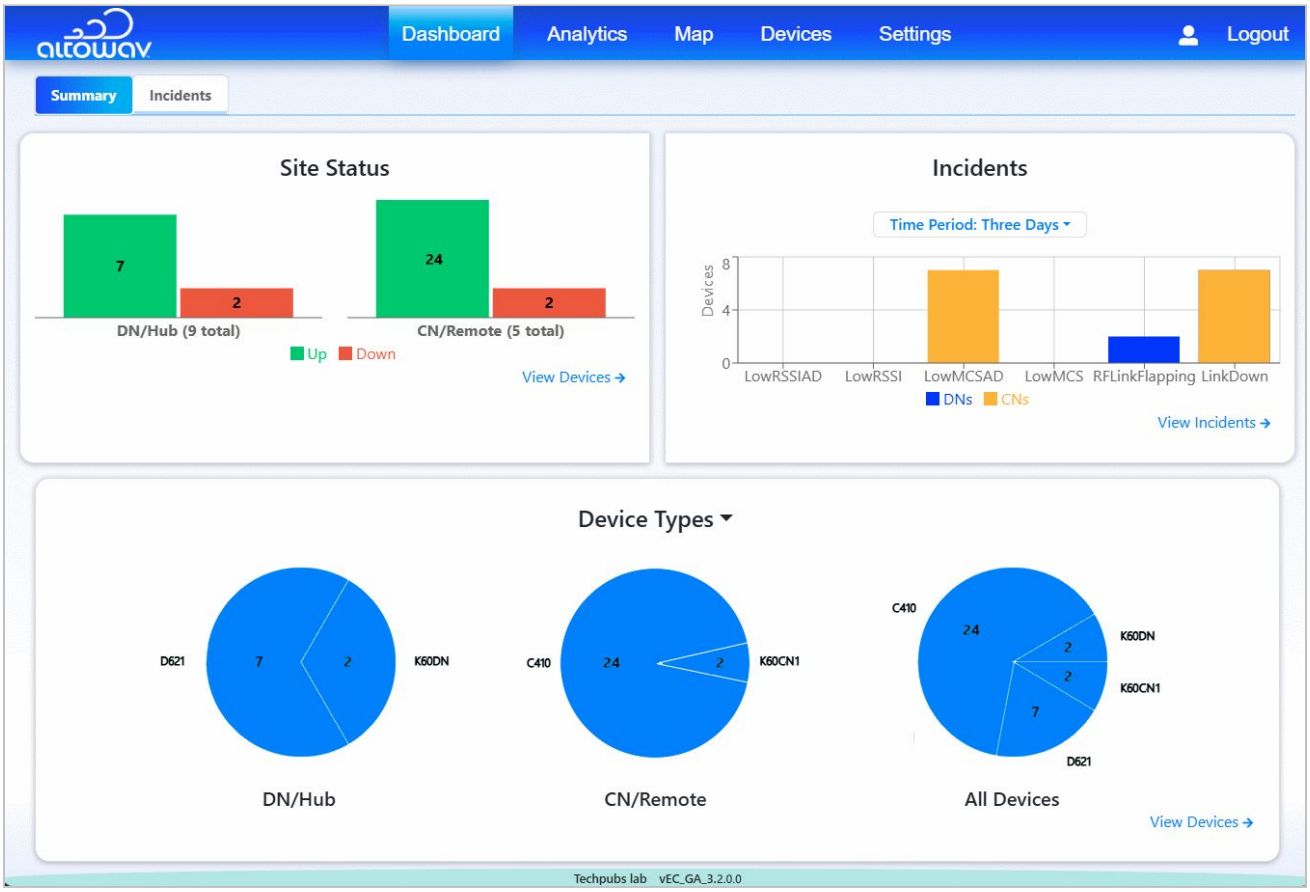
Map -- Shows network topology in a familiar map form. RF channels for links are shown by color. Details of device and link properties are easily viewed. Critical issues such as links down are visually highlighted, enabling you to quickly monitor issues affecting network health.

Devices -- Lists detailed information about devices or links. Many filters available for data and column shown. Menu options enable easy access to device logs, diagnostics, WebUI configuration, device details or quick firmware upgrade.

Settings-- Add or remove devices at the site, including discovery of new devices. Adding/removing devices automatically updates the Map View. Set thresholds for incidents or actions. Manage firmware upgrades. Add or Remove users, control permissions and make firmware available for upgrade.

Dashboard

The **Dashboard** is designed to alert site administrators to potential problems at a site. The **Summary** tab provides a quick overview of site status, current devices and their software versions, and incidents by type over the time period selected.

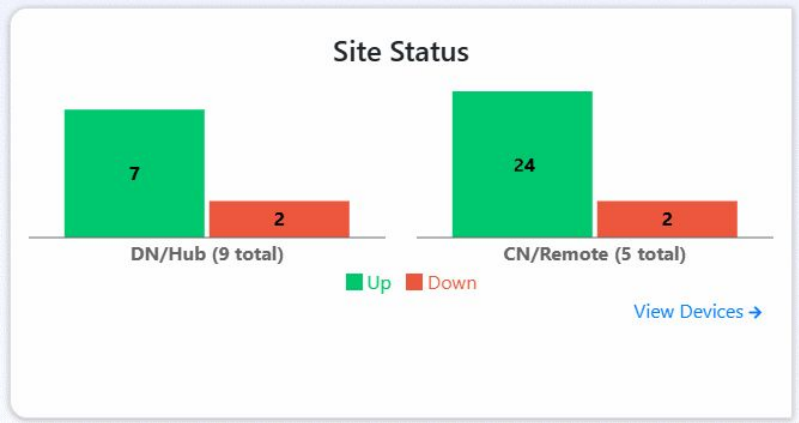


Quick links in each area of the **Summary** show more detailed information about the reported status, incidents and software versions.

- Click **View Devices** to open the **Devices** page.
- Click **View Incidents** to open the **Incidents** tab, useful to determine timing of incidents and and related statistics.
- Click the dropdown in the **Device Types** pane to toggle between **Device Types** and **Software Versions**.

Summary tab - Site Status

Check the **Site Status** pane for the total number of devices and how many are currently up or down.

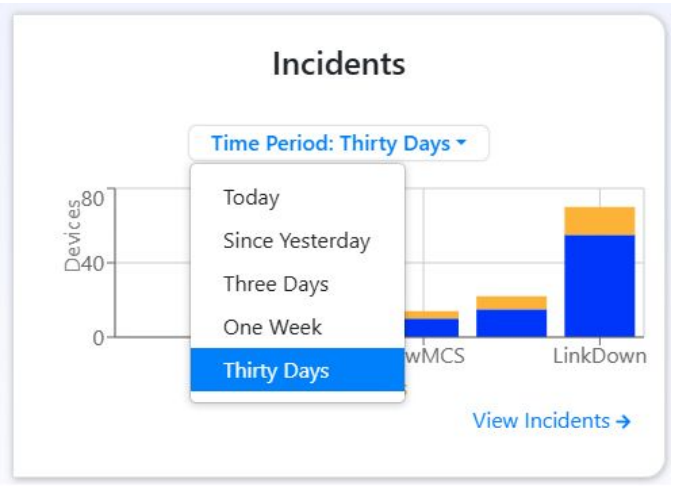


Click **View Devices** to go to the **Devices** page to investigate or resolve problems. The **Devices** page offers many filtering and viewing options, and links to each device's WebUI for configuration.

To check for links that are currently down, go to the network's Map and look for links that are blinking red.

Summary tab - Incidents area

The **Incidents** pane displays incidents from the past day by category.

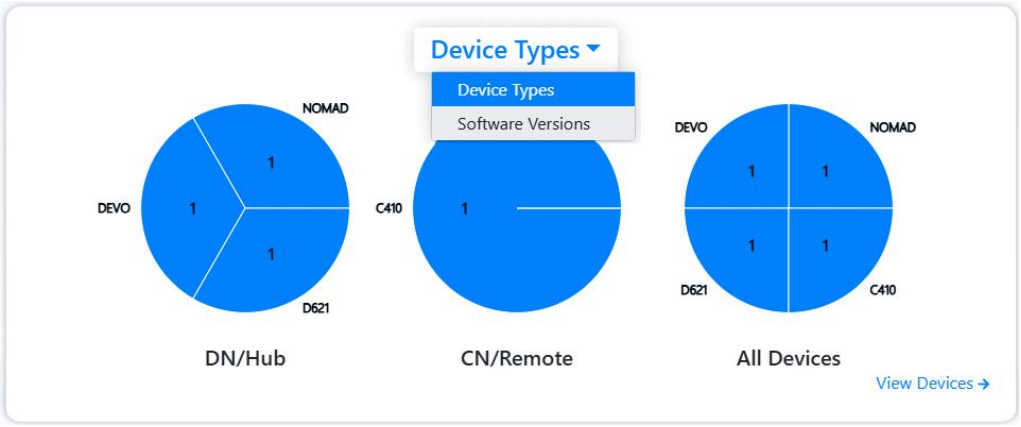


Click **View Incidents** to go to the Incidents tab to show more detail about specific incidents.

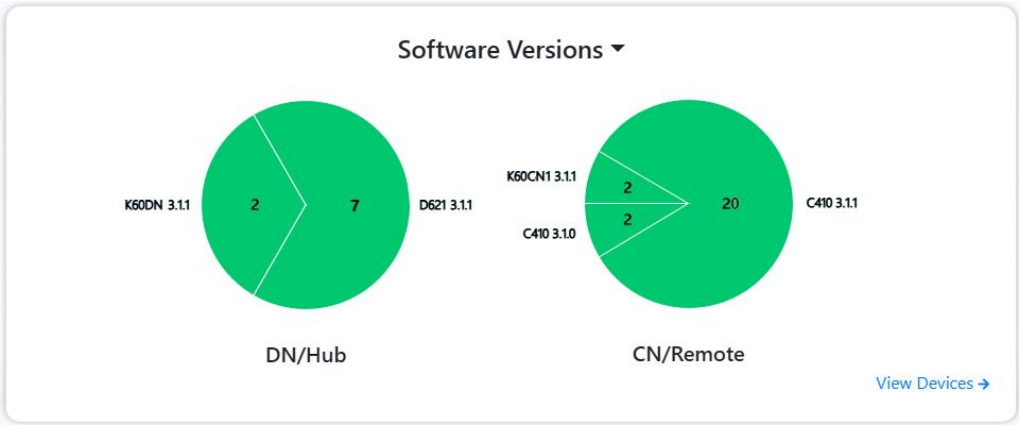
Thresholds for reported incidents can be set in the Thresholds tab of the Settings page.

Summary tab - Device Types/Software Versions

The **Device Types/Software Versions** pane shows the device types.



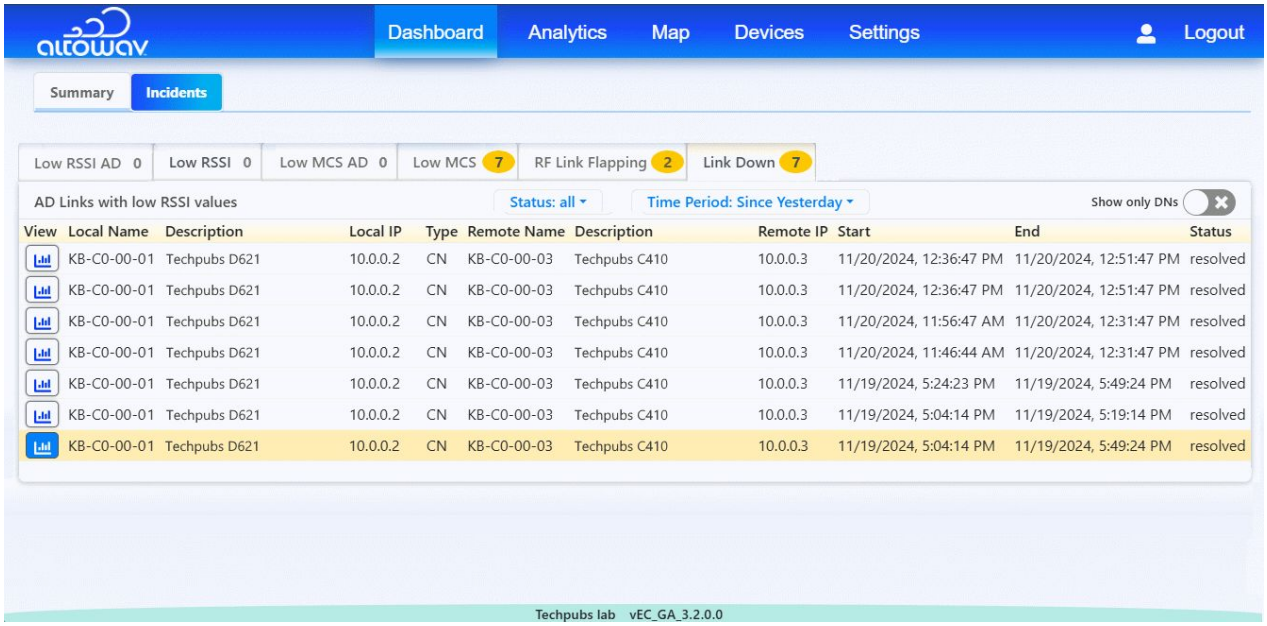
Select **Software Versions** from the dropdown to show the version of the software running on each device.



Click **View Devices** to go to the **Devices** page to identify specific devices with out-of-date software and upgrade them.

Incidents tab

The **Incidents** tab shows specific incident reports and devices involved.



- Incident reports are triggered based on threshold levels defined on the the **Incidents & Actions** tab on the **Settings** page page. See Configure incident reporting for more details.
- Filters allow you to display incident reports based on status (new, recurring, or resolved) and time period, and to only display reports related to DNs.
- Columns identify the local and remote devices involved in the incident, as well as the start and end time of the incident and the status.
- Click the **Graph** icon (📊) next to a incident to display a graph providing further details about the incident.

> **Tip:** Hover over a specific time in the graph to display values at that time. Use this method to view data at the start or end times shown in the Incidents table. See Tips for Viewing Graphs.

Incident type definitions

Different tabs are provided for each type of incident:

Low RSSI — Lists reported incidents when the average RSSI value is less than the configured threshold. Two tabs are available:

- **Low RSSI AD** — Applies to earlier (802.11ad) versions of Altowav products.
- **Low RSSI** — Applies to AltoPlex (802.11ay) products.

Low MCS — Lists reported incidents when the average weighted MCS level is less than the selected thresholds. Two tabs are available:

- **Low MCS AD** — Applies to earlier (802.11ad) versions of Altowav products.
- **Low MCS** — Applies to AltoPlex (802.11ay) products.

RF Link Flapping - The RF link goes down and comes back up more than the configured threshold.

Link Down - Link is reported as down.

Analytics

The page shows traffic and performance data for a device's links. Filters and display options enable viewing data for specific devices or links over a selected period of time. See tips for viewing graphs.

The **Analytics** page has tabs that display graphs or raw data.

Graphs — Shows the data in line graphs of data plotted against time. This, combined with colors and other features of the graphs, enable quick visual assessment of multiple data points at one time.

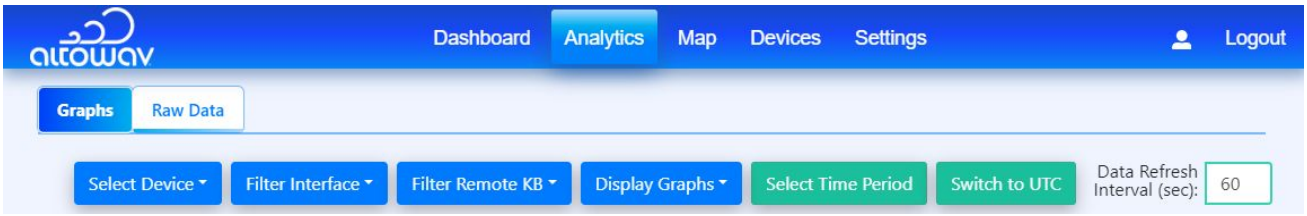
- Download an image (.png) of the graph by clicking the **Document Download** ( ) icon. Downloaded .png files are named by type of graph, device selected date and timestamp. For example: srssi_DN-KB-C6-04-23_Thu, 26 Oct 2023 22_01_59 GMT.png.
- For data older than 30 days, data is down sampled to create graphs. Outliers for this data are retained when creating these graphs. This is done to visually highlight issues, making them easier to find. For example, the weighted MCS values include instances of the lowest MCS, making that issue easier to identify and address. Another example is retaining throughput and power spikes to making those cases easier to trace to specific times and devices.

- See Tips for Viewing Graphs for operational tips.

Raw Data — Shows the data listed in table form, arranged in these categories: Radio Status Data, Radio Status PER data, MCS Histogram Data, MCS Weighted Average Data, Performance Data, Node Identity Data. See Raw Data, for a more detailed description.

Filters

A row of buttons above the data filters what is displayed on the page. Blue buttons filter for device, interface, remote device, and, for the **Graphs** tab, which graphs to display. Green buttons control the time periods shown, including a refresh interval for the display.



> **Tips:** To select specific link(s) to view, start by selecting the device, then filter by interface, and then select the remote device. These selections will stay in place while you select various time periods, select graphs to view, refresh data or move between raw data and graphs.
>
> When a different device is selected, the interface and remote settings are retained if available. Otherwise, they are reset.

A brief description of each of the controls for the **Analytics** page:

Select Device — Select the DN or Hub device on the local side of the link to view. You can view the device list by either **Location** or **Description**. Default: The first device listed.

Filter Remote KB — Select the remote device hostname(s) from the list, **Select All** or limit the remotes to **Only DNs**, (this option appears when both DN and CN links are available). This selection determines which link(s) to graph. Default: **Select all** - All devices linked to the device and interfaces selected.

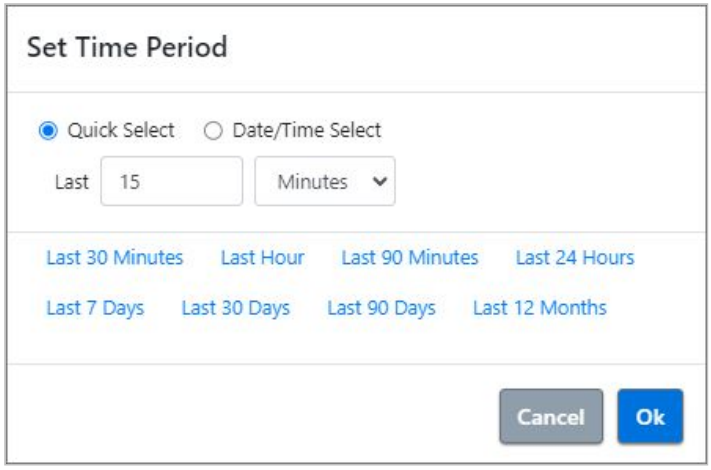
Filter Interface — Select the specific interface(s) on the selected device to graph. This is useful for devices with multiple interfaces, such as the K60DN. Default: **Select all**.

Display Graphs — Select which graphs to view. Settings are retained, until reset by the user. Graphs show the data for the time period selected, except for Node Identity.

- **Node Identity** — Displays information about the selected device, such as MAC address, hardware name, and software version.
- **sRSSI** — Graphs the received signal strength indicator in dBm as polled from devices at the local and remotes of the link.
- **sSNREst** — Graphs signal to noise ratio estimate.

- **TX Power Index** — Graphs the transmission power in dBm as polled from devices at the local and remote ends of the link.
- **RF Channel** — Displays a graph of the RF channel used.
- **Weighted MCS** — Graphs the weighted average MCS for the link.
- **Beam Index** — Displays a graph of the RX Beam Index and of the TX Beam Index for the device.
- **Throughput** — Displays transmission and receiving performance for the link measured in Mb/sec.
- **Block Error Rate (nSyn/nCW)** — Displays a ratio of erroneous blocks to the total blocks transmitted.

Select Time Period — Select the time period to graph. This time period remains selected until a different device is selected or a different time period is selected.



Switch to UTC / Switch to Local - Toggles between displaying analytics in UTC or in local time.

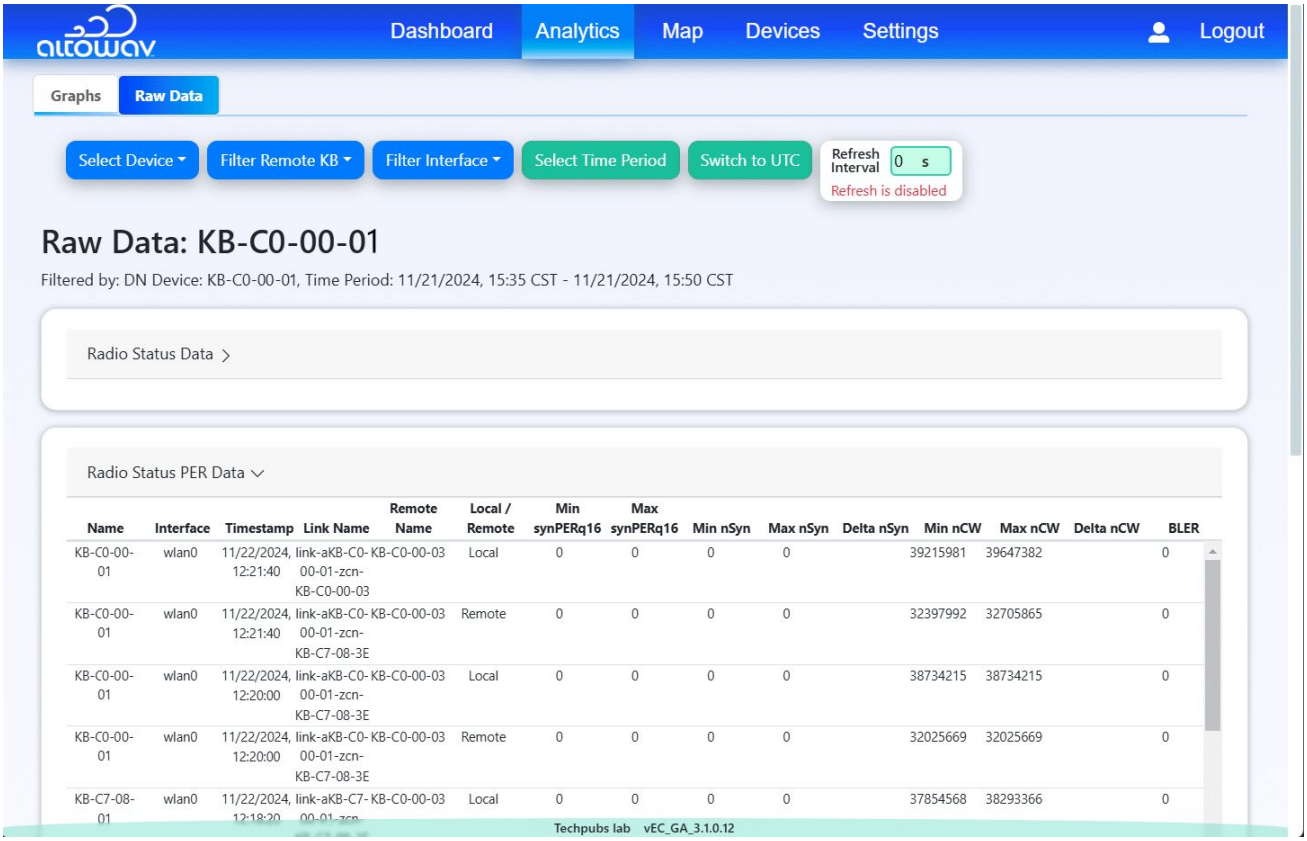
Refresh Interval (sec) - Set the interval for refreshing the graphs. 60 seconds is the minimum refresh interval. Setting the interval to 0 disables data refresh. Default is 0.

Raw Data

The **Raw Data** tab on the **Analytics** page shows polled raw data for a device's link in table format. Categories for raw data include Radio Status Data, Radio Status Packet Error Rate (PER) Data, MCS Histogram Data, MCS Weighted Average Data, Performance Data and Node Identity Data.

The selected DNs, interfaces, remotes and time periods remain the same as you navigate between Analytics graphs and Analytics raw data or refresh the tables. You can adjust the filtering from either page.

Click on the data categories to expand or collapse the data. For example, click on **Radio Status PER Data** to show the packet error rate data from Radio Status, filtered by the device, interface and time selected.

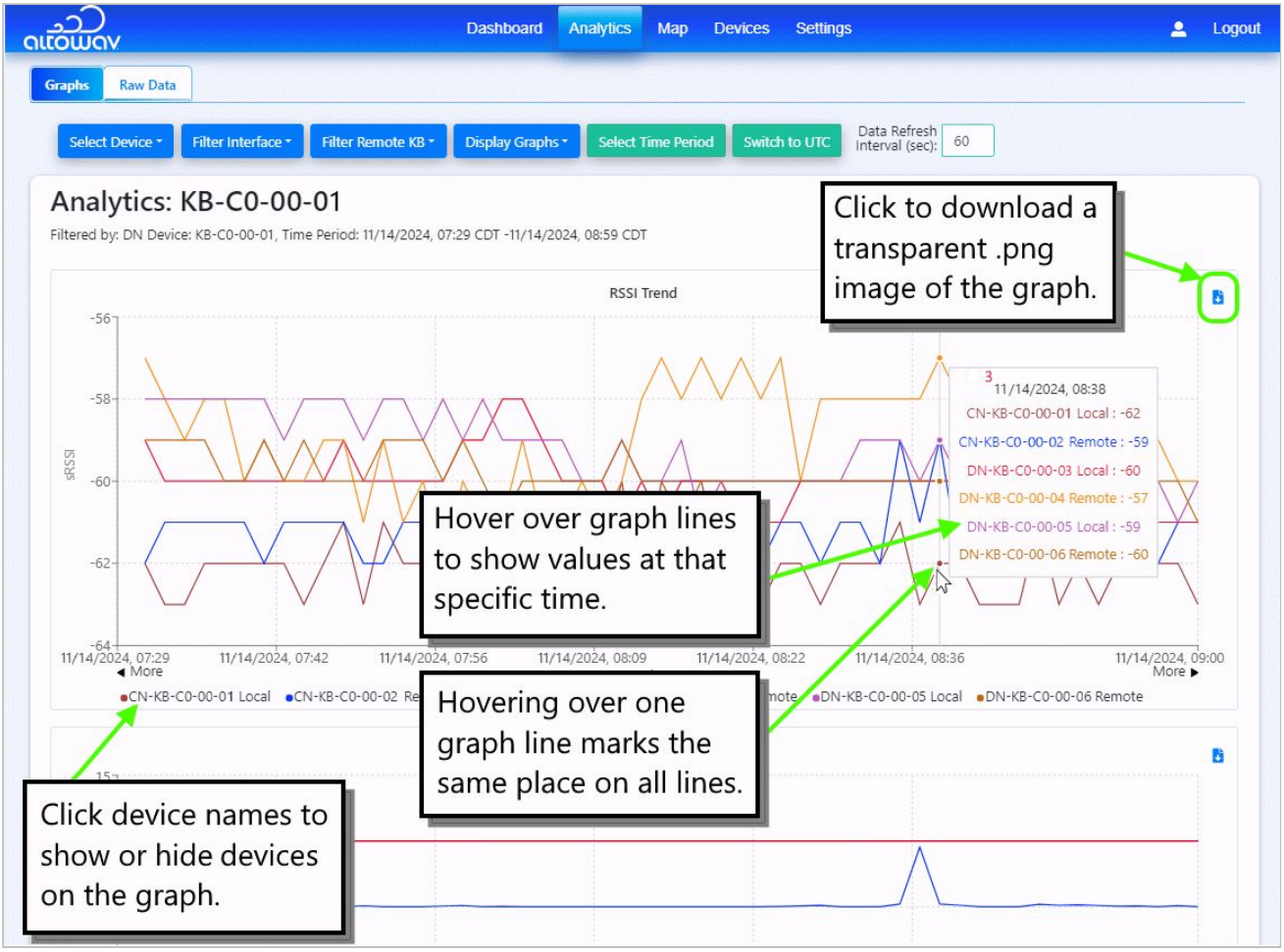


Name	Interface	Timestamp	Link Name	Remote Name	Local / Remote	Min synPERq16	Max synPERq16	Min nSyn	Max nSyn	Delta nSyn	Min nCW	Max nCW	Delta nCW	BLER
KB-C0-00-01	wlan0	11/22/2024, 12:21:40	link-aKB-C0-00-01-zcn-KB-C0-00-03	KB-C0-00-03	Local	0	0	0	0		39215981	39647382		0
KB-C0-00-01	wlan0	11/22/2024, 12:21:40	link-aKB-C0-00-01-zcn-KB-C7-08-3E	KB-C0-00-03	Remote	0	0	0	0		32397992	32705865		0
KB-C0-00-01	wlan0	11/22/2024, 12:20:00	link-aKB-C0-00-01-zcn-KB-C7-08-3E	KB-C0-00-03	Local	0	0	0	0		38734215	38734215		0
KB-C0-00-01	wlan0	11/22/2024, 12:20:00	link-aKB-C0-00-01-zcn-KB-C7-08-3E	KB-C0-00-03	Remote	0	0	0	0		32025669	32025669		0
KB-C7-08-01	wlan0	11/22/2024, 12:18:20	link-aKB-C7-00-01-zcn-	KB-C0-00-03	Local	0	0	0	0		37854568	38293366		0

Raw data listings are useful for cases where a more detailed investigation of performance or operational parameters is required for a specific device, during a specific time period.

Tips for viewing graphs

Analytics graphs have many operational features to help clarify and compare data.



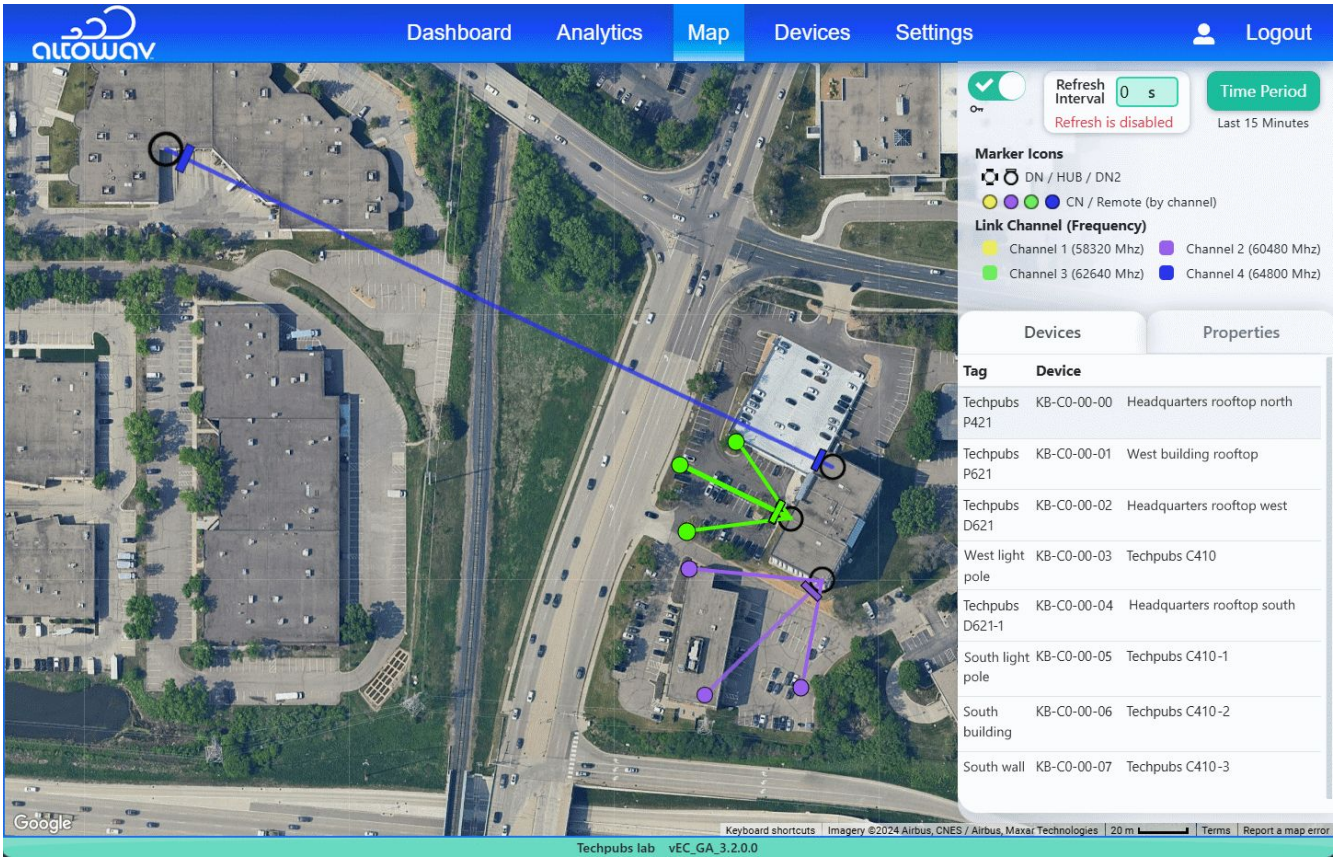
What the names in the legend tell you: The color key below the graphs lists the name of the device on the remote end of the link, (to identify which link each line shows). The name is followed by the word Local or Remote (to specify which end of the link reported the data). For example, **KB-XX-XX-XX Local** graphs data from local side of the link between the selected device and KB-XX-XX-XX. **KB-XX-XX-XX Remote** graphs data for the same link, from the remote side of the link.

Additional operational tips

- Click on the **< More >** at either end of the graph to expand the timeline in either direction.
- Expand a time period shown in the graphs with drag and drop. Drag along x axis to select a time period and drop to expand the graph to that time.

Map

The **Map** page shows the site's network topology in an interactive map. The map uses a Google Maps base with familiar controls for zoom, scroll and switching between map and satellite views.

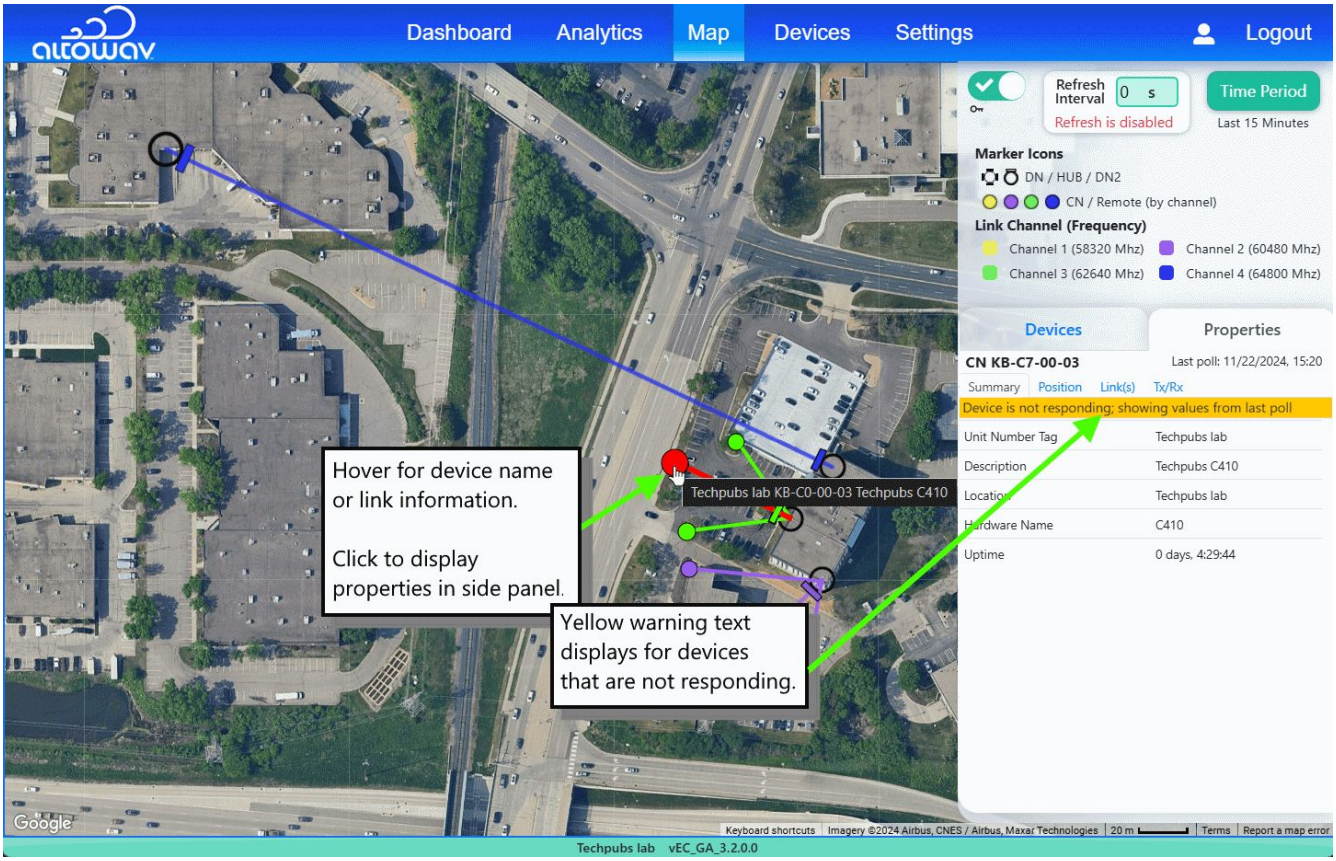


The Map key is at the top of the right sidebar, showing symbols for markers and colors used for each channel. You can hide the key by toggling off the **Key** (🔑) toggle.

Wireless links are shown as solid lines on the map. Channels are displayed in specific colors and down links are displayed in blinking red, to enable quick visualization of real time problems, and which channels are being used in each area.

Click on any device or link for detailed information.

- The **Devices** tab in the sidebar lists all devices with with their tag and hostname.
- Click on a device in the list or on the map to show detailed properties of the device.
- Click on a link on the map to show its properties.

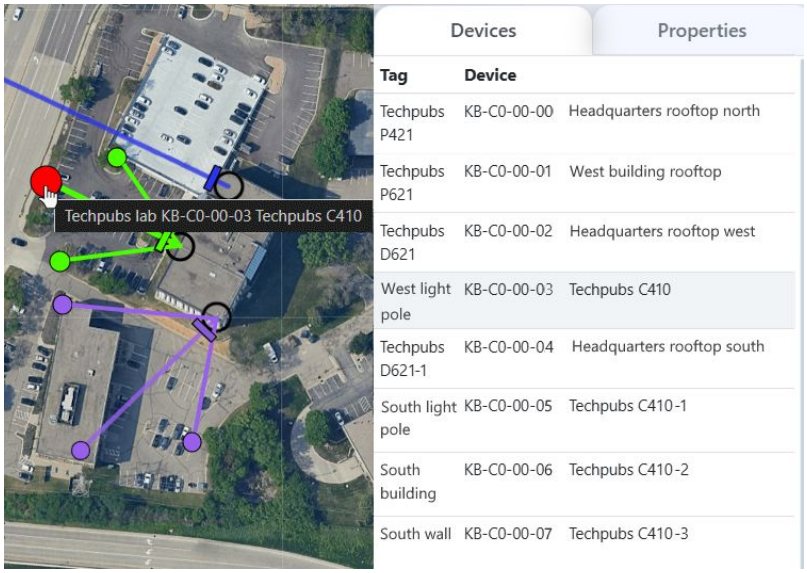


> **Tip:** Device GPS automatically positions DNs on the map, when available. (For Hubs or DNs without GPS enabled, the Map holds the device markers in a tray, until they are dragged to their accurate position.) Markers for connected CN and Remotes are positioned near their connected device. Adjust CN and Remote positions as they are installed to keep the map up-to-date.

The bearing (azimuth) for each DN or Hub should be adjusted manually on the Map, using the compass tool, described in the Properties tab section below.

Devices tab in map sidebar

The **Devices** tab lists all devices shown on the map. Quickly locate a device on the map by hovering over it in the list of Devices - the map marker for the device enlarges. Or, hover over a map marker and the device name is highlighted in the list.



The device's **Tag** is extracted from the device's **Description** or **Location** fields.

- The **Tag** for a DN device is the device's configured description.
- The **Tag** for a CN device is the device's configured location.

See the device documentation for information about how to configure the description and location.

> **Tip:** Consistent information for **Descriptions** and **Locations** will result in an easier-to-use list in this area of the Map.

Properties tab in map sidebar

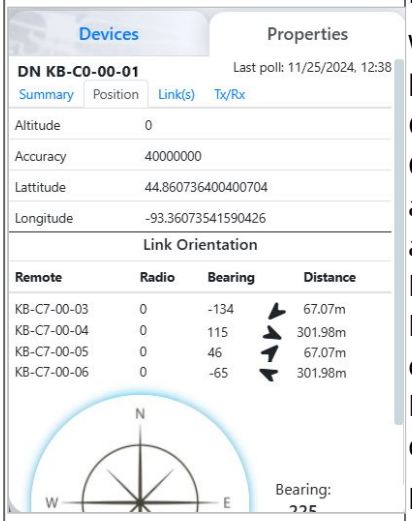
Click on a device in the list or on the map to show its **Properties**. Properties has four sub-tabs, Summary, Position, Link(s) and TX/RX throughput.

Summary

DNs — Switch point tag, Description, Location, Hardware Name, Uptime and temperatures for the case and processor.

CNs — Unit Number Tag, Description, Location, Hardware Name and Uptime.

K60, K60c — Switch point tag (Hub), Unit Number Tag (Remote), Description, Location, and Uptime.



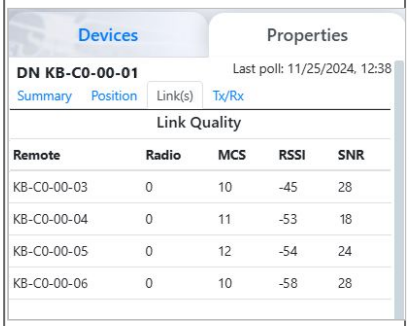
Position

DNs — GPS values for Altitude, accuracy, latitude, and longitude are shown. Link Orientation information is bearing and distance information taken from the map. The links listed are from the DN's configuration. They may be active or inactive.
Drag the circle on the compass to manually adjust the DN's Device Bearing. Use the orientation for Radio 0 to set bearing.

When a DN marker is manually repositioned on the map, a **Reset** button appears. Click it to move the marker to the device's polled GPS location.
CNs — GPS values for Altitude, accuracy, latitude, and longitude are shown if available. Otherwise, Latitude and Longitude are listed as shown on the map. Drag the marker to the actual client location. Link Orientation is shown for the each K60CN1, including the Remote name, link interface, bearing and distance. These values come from the relative positions of the K60CN1 and its linked K60DN on the map. They can be manually changed by dragging the devices.

K60, K60c — Latitude and Longitude are listed as shown on the map.

Link Orientation information is bearing and distance information taken from the map. Drag the marker to the actual location. Links listed are from the K60's configuration. They may be active or inactive.
For Hub devices only, drag the circle on the compass to manually adjust Device Bearing.



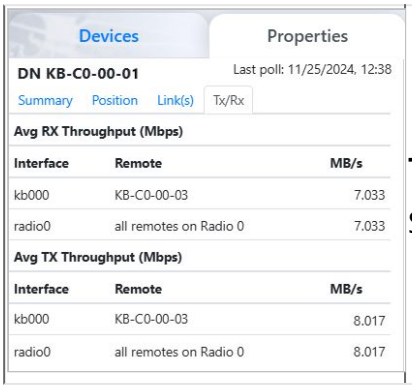
Link(s)

DNs — Remote devices, Radio interface, MCS, RSSI and SNR for each link.

CNs — Remote DN, Remote MAC, RF Channel, Power, MCS, RSSI, SNR, Link Uptime, Link Up Attempts, Link Up/ Data down statistics, RX Beam Index, TX Beam Index, Link Name and Link Description.

K60 - Hubs list remote names, MCS, RSSI and LinkQ are shown for each link.

Remotes list the Remote Hub, Channel, TX Beam Index, RX Beam Index, MCS, RSSI and LinkQ are listed.



TX / RX

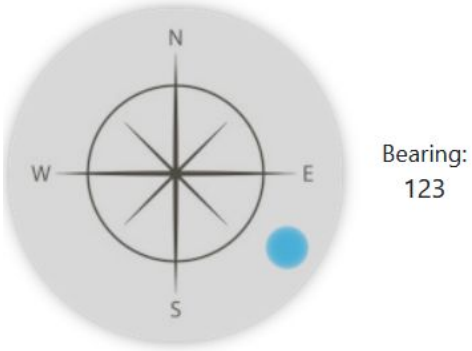
Shows throughput statistics for all interfaces on the device.

Adjustments for Map accuracy

Whether setting up an initial network or adding / removing devices, adjusting devices' positions and bearings enhances the accuracy and usefulness of the Map. Common adjustments per device type:

DN or Hub devices

- For devices with GPS disabled or unavailable, drag the device from the tray to the installed location on the map. Devices with active GPS are automatically positioned at their GPS location.
- Use the compass on the **Properties > Position** tab to set the azimuth per the actual installation. Drag the circle on the compass to the device's actual azimuth. For K60DNs, use the Radio 0 azimuth.



CNs or Remote devices

Map markers for the K60CN1s or Remotes are added to the map near the DN or Hub to which they connect. Drag the K60CN1 markers to their actual installed location on the map.

K60CN1s at initial location on Map.

K60CN1s dragged to actual locations.

Add new devices to the Map

Adding a new device to the network site also adds it to the Map. How a device is added to the network varies by type of device. For detailed examples see the Add a CN or Remote to the Network or Add a DN or Hub to the Network sections of the Common Administrative Tasks topic. Brief examples of how the devices are added to the Map and positioned are given below.

Adding CN or remote devices

CN or Remote devices are added to the Map as they are installed and connected to the network. Examples:

CN Example: Installing and connecting the CN to a DN in the network (adding it to the **CN responder** on the DN), adds the CN to the map. If the CN's GPS is disabled, or if it is a K60CN1, it is added close to its connected DN and should then be repositioned to its actual location on the map.

Remote Example: Installing a Remote which connects to a Hub in the network, adds the Remote to the map, close to the Hub's location. The Remote should then be repositioned to its actual location on the map.

Adding DN or Hub devices

DN or Hub devices can be manually added to the network from the Settings page: Click the **Site Devices** tab. Click **Add Device**. Enter the **IP Address**. Then, **Save Changes**.

DN devices, (not Hubs), can also use auto discovery from the **Settings** page: Click the **Site Devices** tab. Click **Device Discovery**. Wait for the device to be added to the list. Then **Save Changes**.

With either method, devices with GPS enabled will be auto-positioned on the map. Devices with GPS disabled or unavailable will be placed in the device tray for manual positioning.

Removing devices

Device data is retained by AltoCommand for 90 days after the device is removed.

When a device is physically uninstalled from the network or powered down, its map marker turns yellow, indicating it is unreachable. Popup information for links to the unresponsive unit will also display yellow highlighting.

To remove a DN or Hub from the network map, delete it from the Site Devices list on the Settings page. Adjust the DN Responder configuration for the removed DN.

To remove a CN from the network map, delete it from **CN Responder** list on the linked DN.

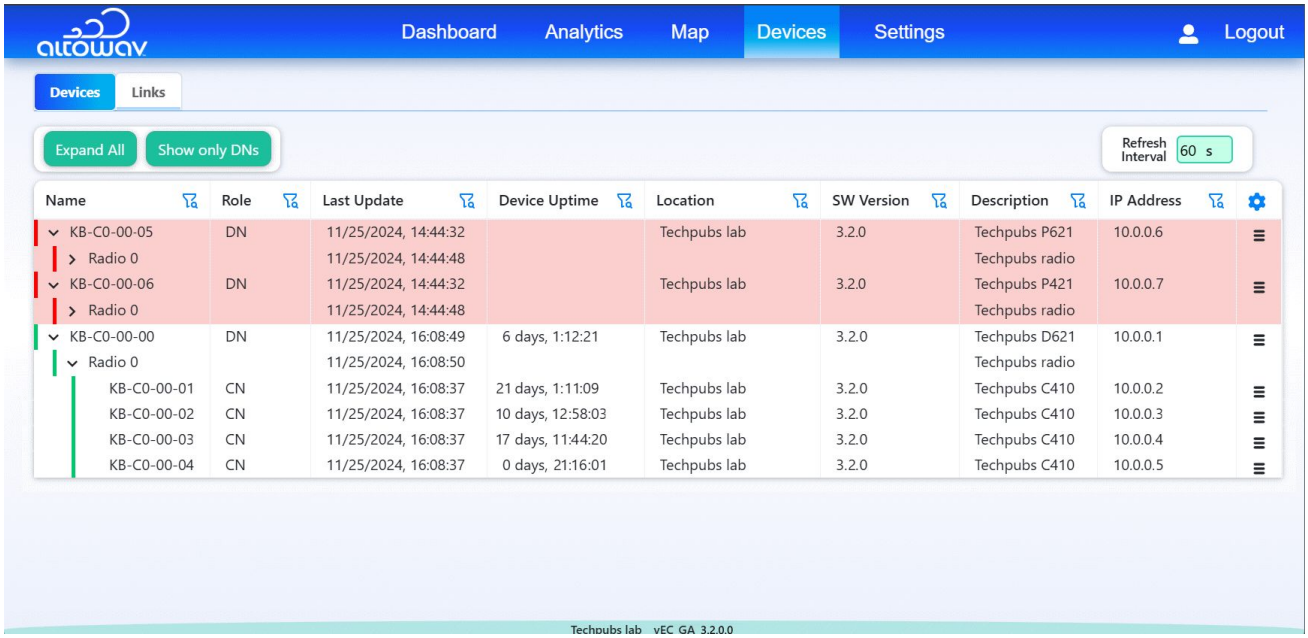
To remove a Remote from the network, uninstall it, power it down, or reconfigure it to be unreachable.

Devices

Click **Devices** in the top navigation bar to go the Devices and Links tabs. These tabs show a quick assessment of the current issues in the overall network, enabling you to spot areas of concern and dig deeper for information about devices and links.

Devices shows a snapshot of device status using color to highlight issues.

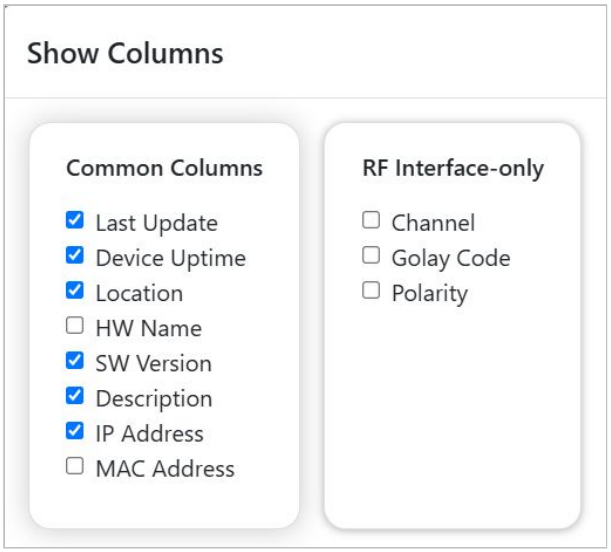
- A green bar (I) at the start of a row shows a healthy device and link, normal operations.
- A red bar (I) at the start of a row indicates an issue with a device or link for the device. (Note, a poll can be missed for many reasons, connectivity issue, slow network, the polling timed-out, etc. so the issue may be temporary.)
- Light red highlighting on a row shows the device or sector with the broken links or reachability issue.



Columns show brief descriptive information about each unit. Click a column heading to sort it by ascending (▲) or descending (▼) order.

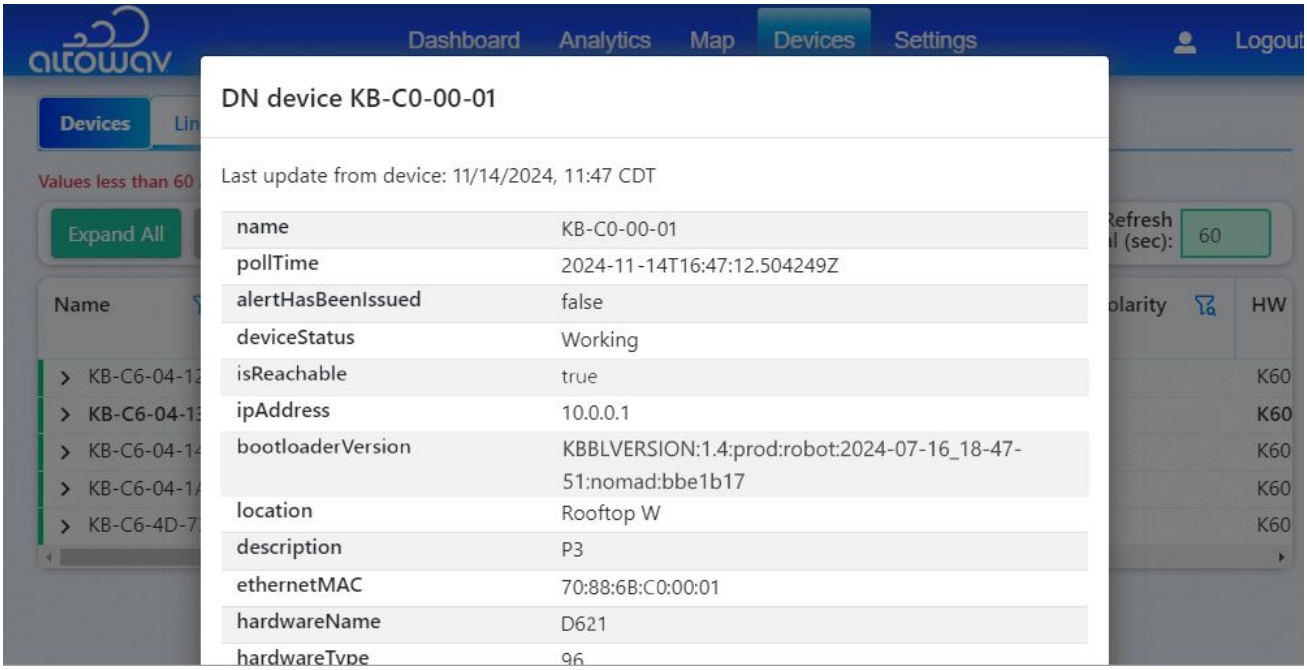
Note: For the K60DN, each of the device's radio interfaces (Radio 0-3) are listed as wlan0-wlan3.

To select which columns to display, click the **Settings** icon (⚙).



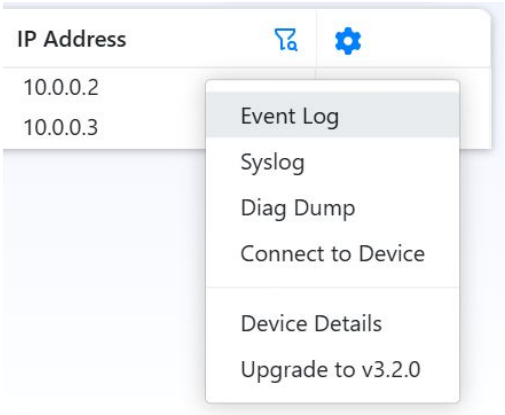
Click › to expand or ⌄ to collapse the list of the device's interfaces and linked devices.

Click on any row to show more information about the device on that row. Copy/paste information as needed. Click anywhere outside the info box to close it.



For any unreachable devices, the timestamp for the last connection is listed.

To investigate an issue more closely, generate and download more data or access a device's WebUI from the options menu (☰) at the end of the device's row.



Event Log — Subset of available information from device Syslog, showing events for the device.

Syslog — Complete log of information available from device.

Diag Dump — A diagnostic file captures historical information about the device operations and interactions. It is intended for troubleshooting issues. This is particularly useful when contacting Altowav with a question or issue.

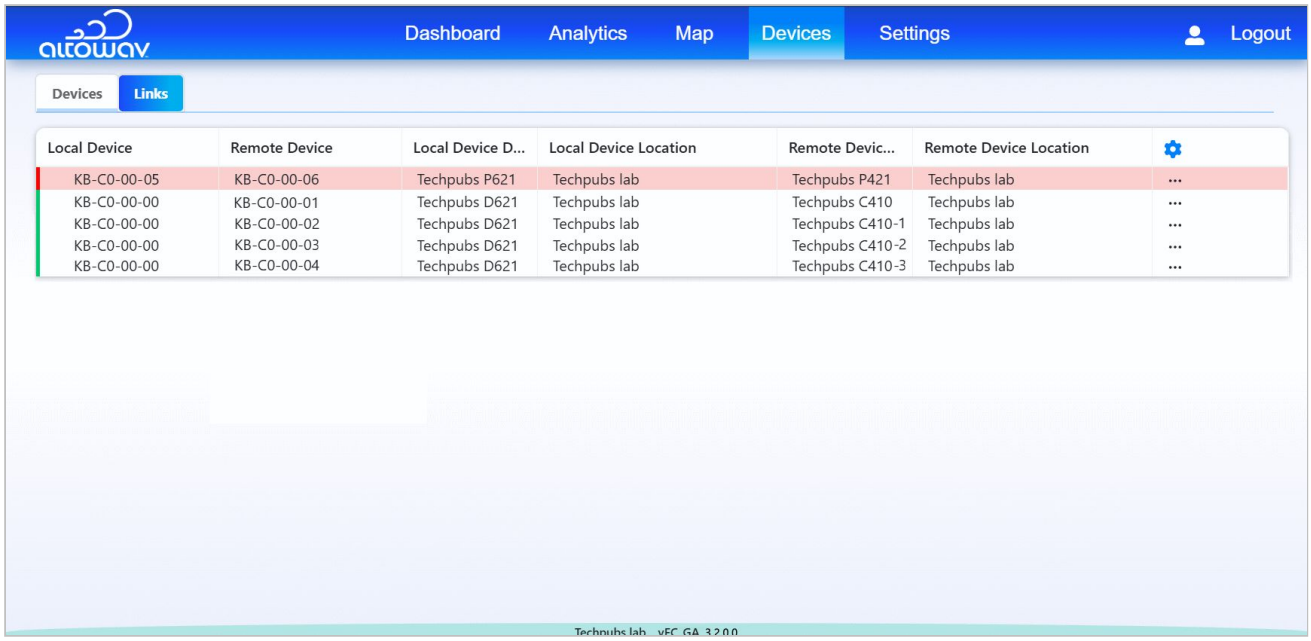
Connect to Device — Opens the WebUI for the device. Login is required to do anything more than view Status information.

Device Details — Shows more information about the device, a radio interface, or connected device.

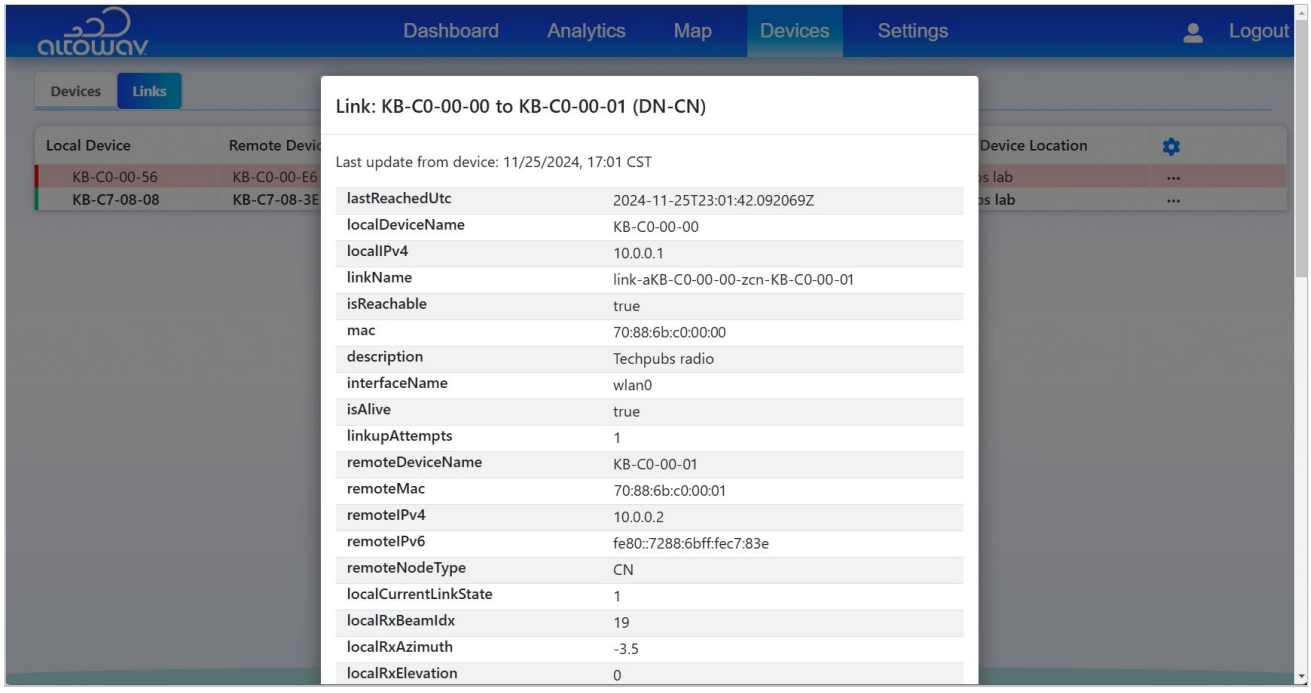
Upgrade Firmware — Offers a quick way to upgrade to the Target Firmware version. See Firmware_settings.

Links

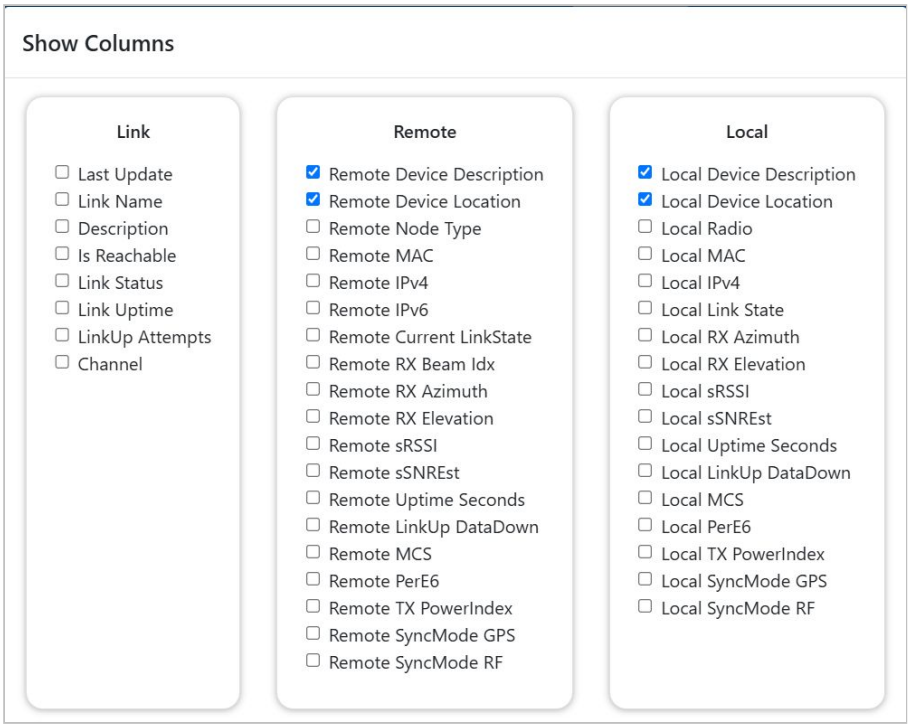
The Device Links tab shows all links in a sortable table. Click on any column head to toggle through sorting options. Resize columns, as desired by dragging the edges of the column heads.



Click on any row to display details about the link. Click outside the info box to close it.



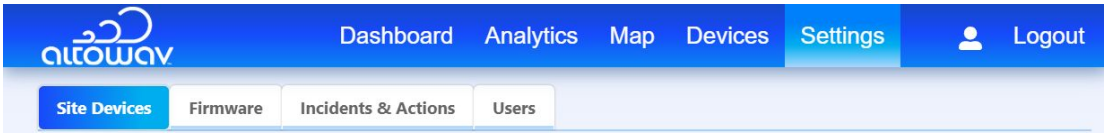
Click the **Settings** icon (⚙) to select which columns are displayed.



The **More Options** menu (•••) at the end of each row has options to **Reform Beam** for the link, or show **Link Details**.

Settings

Use the **Settings** page for initial network setup, to manage site devices, to add firmware for device upgrades, to set incident thresholds, and to manage users and permissions.

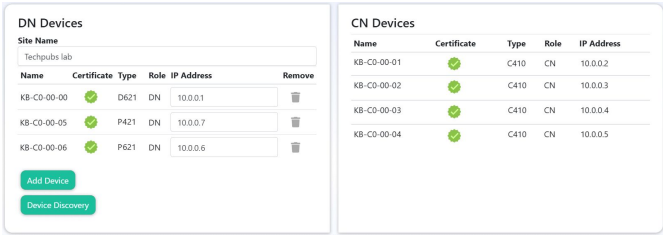


Manage site devices

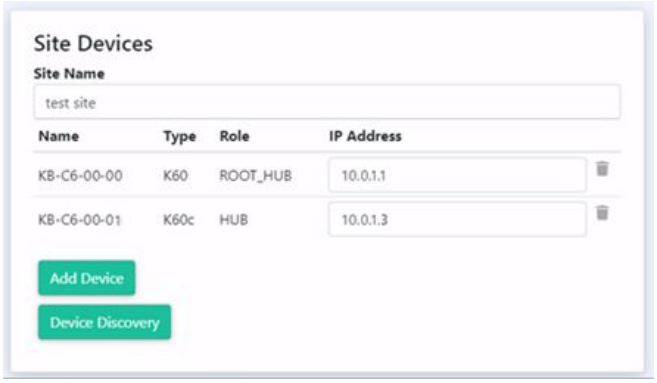
Use the **Site Devices** tab to perform the initial setup of the network, authenticate devices for use with the AltoCommand, or to review or update devices.

Initial setup can be as simple as adding one DN manually, then using **Device Discovery** to add all other DNs. Or, DNs and Hubs can be added manually. See Set Up a New Network.

Site Devices - AltoPlex Devices



Site Devices - Hub Devices



Use **Site Devices** to do the following tasks.

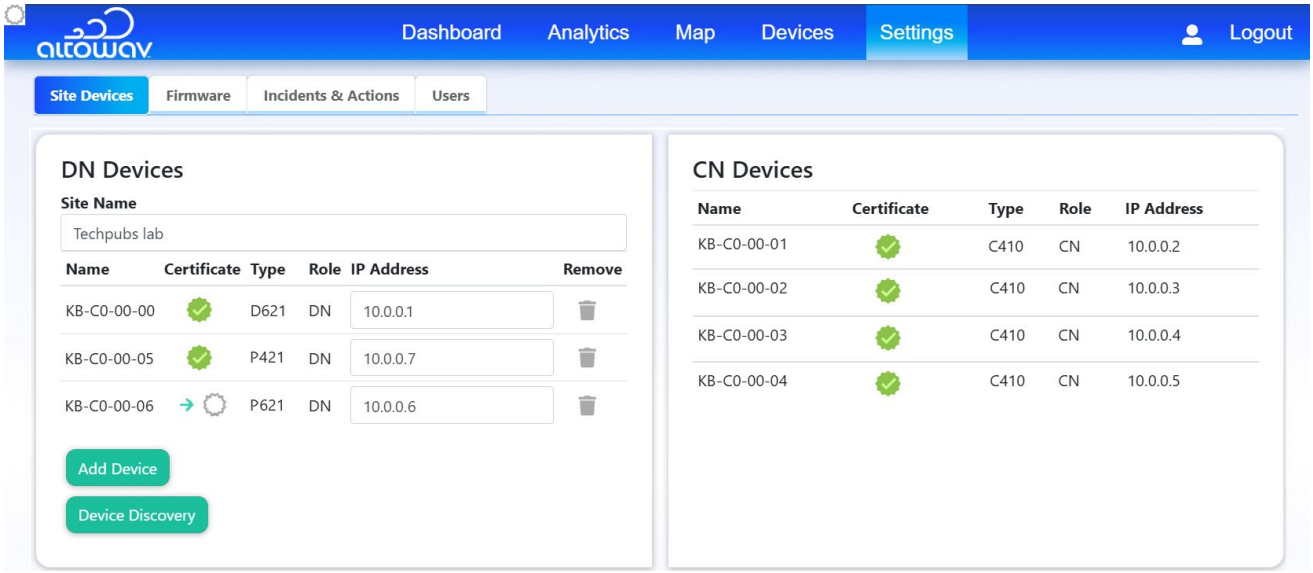
- Initial network setup. See Set Up a New Network for step-by-step instruction for initial network setup.
- To remove a device from the network site, click on its **Delete** icon (🗑).
- Manage authentication between the device and AltoCommand.
- To discover newly added DNs, click **Device Discovery** at any time. If a DN is installed, but not connected to the network, it will not be discovered.
- To manually add a new DN or Hub to the site, click **Add Device** and enter its IP address. Then click **Save Changes**.

Device authentication

AltoCommand requires authenticated access to AltoPlex devices in order to be able to perform write operations to the device, including firmware upgrades and the automated rebeamforming

feature. When a device is authenticated with AltoCommand, an authentication certificate signed by AltoCommand is installed on the device.

Note: Authentication does not apply to the K60, K60c, K60c+, K60i, and K60x devices products. As a result, AltoCommand only has read access to these devices.



To install an AltoCommand certificate on the device:

1. In the **Certificate** column, click the icon next to a new device.

   AltoCommand will install a certificate on the device. When the certificate installation is complete, the icon will change to .

2. Repeat for each device.

After a device has been successfully authenticated, it will have a green checkmark in the **Certificate** column. Various other icons in the **Certificate** column have other meanings:

Icon	Meaning	Remediation
	Authentication is successful.	
	Authentication failed.	Click the icon and select **Try again**.
	Authentication has not been performed.	Click the icon to begin the authentication process.
	Authentication is in an unknown state.	This could be the result of a device being offline or unreachable.
	Device is already authenticated with another instance of AltoCommand.	Delete the existing client certificate on the device and perform the authentication again.

Delete an existing client certificate

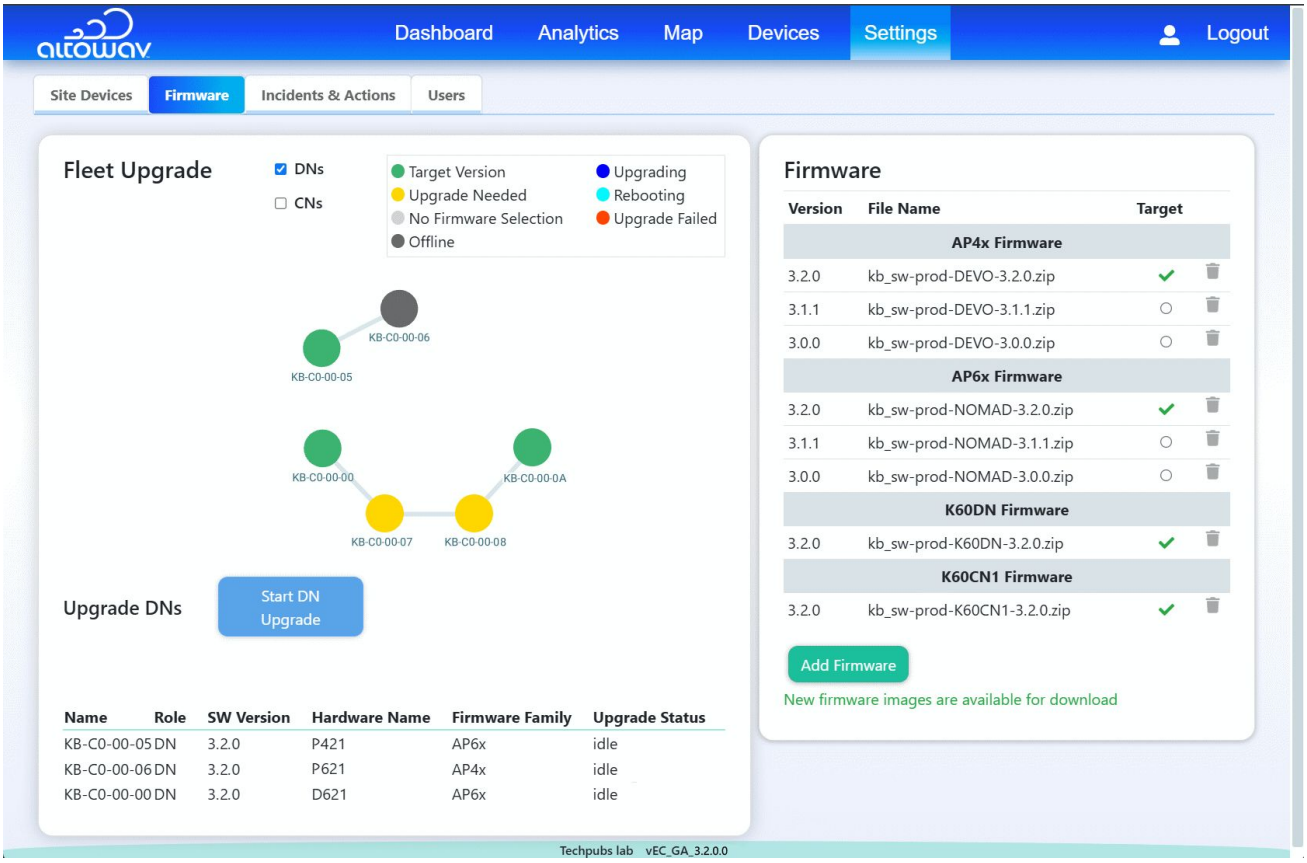
It may sometimes be necessary to delete an existing client certificate. This can be done one of two ways:

- Factory reset the device. See device documentation for instructions.
- Use the install_client_ca_certificate?reset=true REST API, for example:

```
$ curl \
https:// <server_name>/rest/v002/security/install_client_ca_certificate?
reset=true \
-X POST \
-d ""
```

Firmware settings

Use **Settings** > **Firmware** to quickly review upgrade status or run an automatic upgrade, add new versions of device firmware, and select a target version to use for quick upgrades.



Note: Upgrade from within AltoCommand is only available for AltoPlex devices. You cannot upgrade K60, K60c, K60c+, K60i, and K60x devices from within AltoCommand.

Fleet Upgrade pane

The **Fleet Upgrade** pane provides a visual display of the current state of firmware versions in your network, as well as a way to quickly upgrade all DNs or CNs in your network. Devices are color-coded based on the firmware installed on the device and the firmware version selected as the target.

The **Fleet Upgrade** pane defaults to displaying all DNs in your network. Click CNs to display firmware version for client nodes in your network.

Firmware pane

The **Firmware** pane lists all firmware currently available on your instance of AltoCommand. In this pane you can set the target firmware level for each type of device, as well as adding and deleting firmware versions from your instance of AltoCommand.

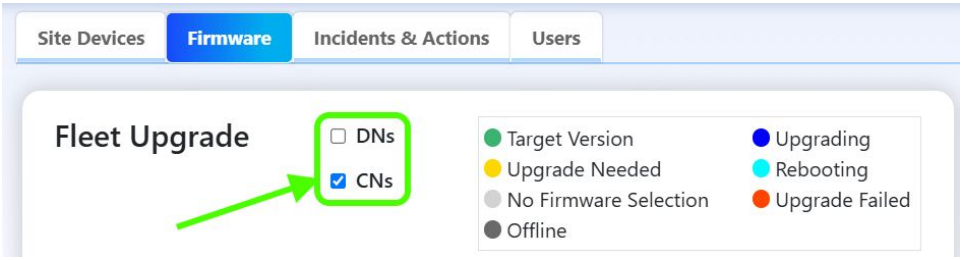
Upgrade all devices to the target firmware version

Note: Since upgrading devices interrupts operation for a short period of time, Altowav recommends this be done at low traffic times, with active monitoring.

1. With the **Fleet Upgrade** pane displaying all DNs in your network, click **Start DN Upgrade** to automatically perform an upgrade of all distribution nodes that are not at the target firmware version.

   Monitor progress until the upgrades are complete.

2. When the upgrade of distribution nodes is complete, click **CNs** to display all client nodes in your network.



3. Click **Start CN Upgrade** to automatically perform an upgrade of all client nodes that are not at the target firmware version.

   Monitor progress until the upgrades are complete.

Add firmware

To add firmware versions to your instance of AltoCommand:

1. Click **Add Firmware**.

2. In the resulting dialog, click the **Download** icon (⬇) to add a firmware version to your instance of AltoCommand.

   Firmware is selected based on the device family. See Firmware device family for further information.

3. Click **Close**.

Set target firmware

Target firmware is the version used for the **Quick Upgrade** option on the Devices page and the automatic upgrade in the **Fleet Upgrade** pane.

To select a firmware version as the target version, click on its radio button in the **Target** column of the firmware list. Clear the Target setting by selecting a different version or by deleting the target version.

Target firmware is based on the device family. See Firmware device family for further information.

Firmware device family

AltoPlex firmware is provided for four device families:

- **AP6x** — Firmware for the D621 and P621 devices.
- **AP4x** — Firmware for the P421, C420, and C410 devices.
- **K60DN** — Firmware for the K60DN.
- **K60CN1** — Firmware for the K60CN1.

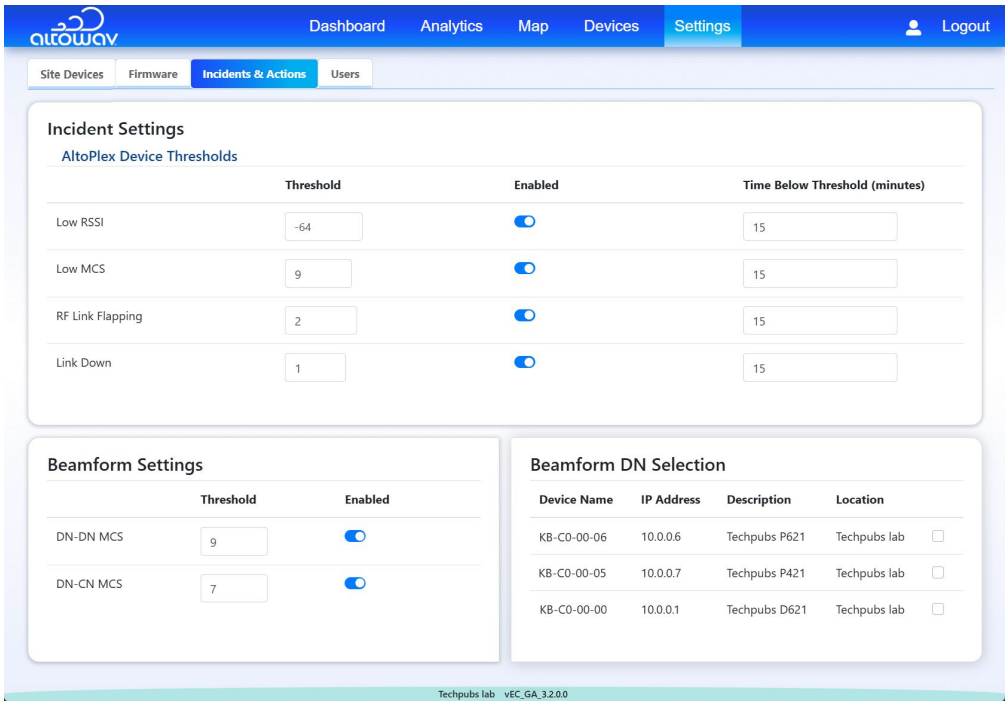
> **Tip:** The **Fleet Upgrade** pane lists the firmware family for each device.

Remove firmware

To remove a version of firmware, click the **Delete** icon (🗑) at the end of the row.

Incidents and Actions

The **Incidents and Actions** tab is used to set threshold levels that trigger incident reports and to configure rebeamforming activities.



Configure incidents

The **Incidents Settings** pane is used to configure incident reporting by enabling/disabling incidents, as well as setting thresholds and intervals. The following incidents are available for configuration:

Low RSSI — RSSI (Received Signal Strength Indicator) is a measurement of how well a device can receive signals from external wireless devices. The higher the number, the better the signal strength. By default, when the average RSSI for a device is below -64 dBm for 15 minutes, an incident report is logged and displayed on the **Incidents** tab of the **Dashboard**.

Low MCS — MCS (Modulation Coding Scheme) is a measurement of how efficiently data is being transferred over a wireless connection. AltoPlex devices use a weighted MCS value of 2-12. By default, when the average weighted MCS of a device is below 9 for 15 minutes, an incident report is logged and displayed on the **Incidents** tab of the **Dashboard**.

RF Link Flapping — Link flapping refers to a link that goes down and comes back up. By default, if a device has two link flapping incidents in a period of 15 minutes, an incident report is logged and displayed on the **Incidents** tab of the **Dashboard**.

Link Down — By default, if a link is reported as down for 15 minutes, an incident report is logged and displayed on the **Incidents** tab of the **Dashboard**.

See Configure incident reports for further details.

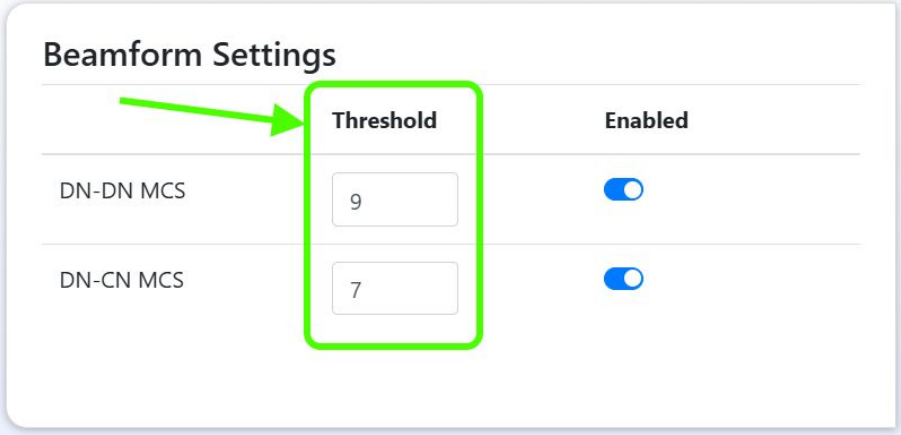
Note: Incident threshold settings are only available for AltoPlex devices. This feature is not available for K60, K60c, K60c+, K60i, and K60x devices.

Automated rebeamforming

Rebeamforming is a process by which a wireless connection between two devices is taken down, and a new connection is formed. The default behavior for Altowav devices is to periodically reform beams every four hours, regardless of the quality of the beam.

With AltoCommand, you can disable periodic rebeamforming and use an automated rebeamforming mechanism instead. With automated rebeamforming, AltoCommand performs rebeamforming based on configured MCS threshold values.

The MCS threshold value represents the average weighted MCS, sampled every 60 seconds, over a period of one hour.



- When a wireless connection is performing above the configured MCS threshold value, rebeamforming will not be performed.
- When the connection falls below the configured threshold, rebeamforming will be performed automatically.
- After a link is reformed, AltoCommand will wait two hours to rebeamform again, regardless of the quality of the link.

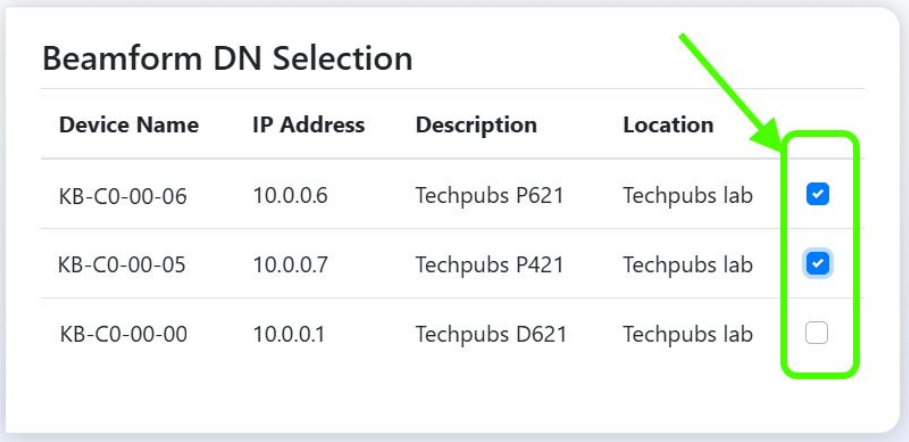
If a wireless connection is regularly being rebeamformed by the automated rebeamform feature, the line of sight between the two devices should be inspected to determine if there are any physical obstructions that may be causing the link to have poor performance. Alternatively, you can disable automated rebeamforming on devices with problematic links; however, this will reenable the device's periodic rebeamforming.

You can also set different values for links between two DNs, and links between a DN and a CN, to accommodate situations where lower-performing links between DNs and CNs is acceptable.

Note: Beamform threshold settings are only available for AltoPlex devices. This feature is not available for K60, K60c, K60c+, K60i, and K60x devices.

Enable automated rebeamforming

- If the configured MCS settings for DN and CN links are appropriate for your network, in the **Beamform DN Selection** pane, enable automated rebeamforming by clicking the checkbox at the end of the row for each applicable device.



- To change the MCS threadhold values:
  1. In the **Beamform Settings** pane, type appropriate the MCS values for both DN to DN and DN to CN links. Allowed values are between 2 and 12. This figure represents the average weighted MCS, sampled every 60 seconds, over a period of one hour.
  2. Toggle off **Enabled** to turn off automated rebeamforming for either DN to DN or DN to CN links.

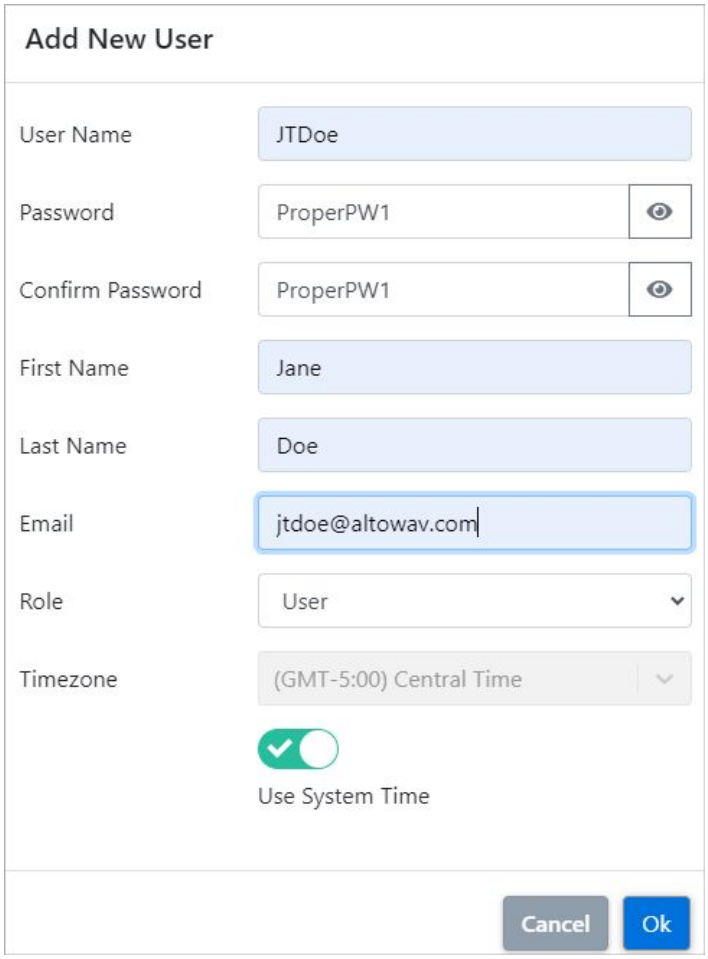
Manage Users

Add and delete users from the Users tab of the Settings page.

Add New User

Admin permissions are required to add a new user.

1. Click **Add User**.
2. Enter the requested user information and select a role (User or Admin) for the User and time zone.



   For **Role**, select either **Admin** or **User**.

   - Users with the **User** role have read-only access to AltoCommand, with the exception that they can edit their own user information and change their password.
   - Users with the **Admin** role can perform write operations within this instances of AltoCommand.

3. Click **OK**.

Altowav recommends that new users change their password for general security.

Delete a user

Admin permissions are required to delete a user.

To remove a user, click the **Delete** icon (🗑) at the end of the row.

Related topics:

AltoCommand Installation - Install the AltoCommand.

Set Up a New Network - Name the site and initially populate the Site Devices list.

Add a CN or Remote to the Network - Includes tips for adjusting marker positions.

Add a DN or Hub to the Network

Change Password

Lost Password

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-C0-00-00.

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

FWA — See Fixed wireless network.

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

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

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

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

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

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

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

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

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

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

P2P, **PtP** — See point-to-point.

PtMP, PMP — See point-to-multipoint.

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

PoP — See point of presence.

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

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

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

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

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

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

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

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