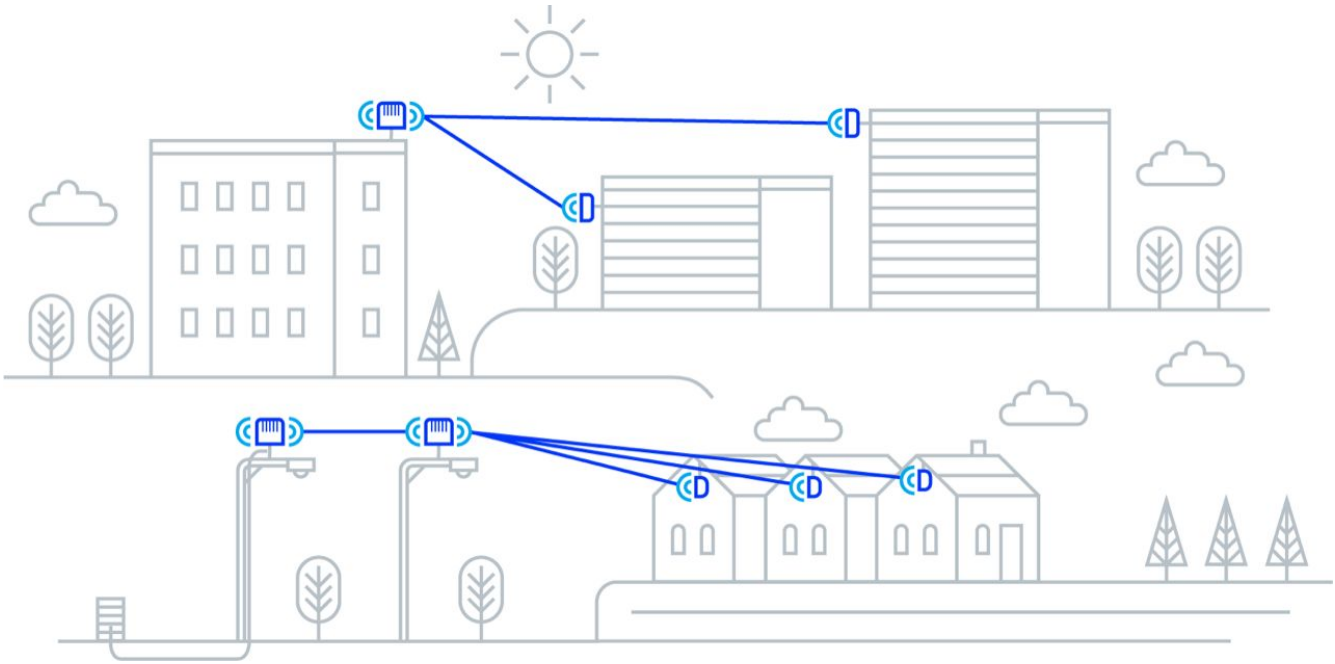


AltoCommand User Guide

October 21, 2025

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

Revision	Date
Release of AltoCommand version 4.0. Includes: • Support for AltoCommand in the Cloud. • Device connections are now: ◦ Initiated on the device. ◦ Accepted on AltoCommand after initiation on the device. ◦ Reverse tunnel established between AltoCommand and the device. • Support for one or more Networks within a single instance of AltoCommand. • A **Temperature Trend** graph has been added to the **Analytics** page.	10/21/2025
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 using AltoCommand software, both in the Cloud and on-prem versions, for initial setup, monitoring, and optimization, as well as common management tasks such as fleet-wide device upgrade.

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 and 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, and is designed to provide management of Altowav networks and individual devices that off-the-shelf tools cannot deliver.

AltoCommand is available in two formats: A subscription-based instance running in the cloud, or pre-installed on a fanless industrial PC designed to operate in your on-prem network.

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 Received Signal Strength Indicator (RSSI), poor Modulation Coding Scheme (MCS), link flapping, and disconnected links.
  - Types and number of devices in your network.
  - Firmware version compliance.
  - Device authentication status, to allow authenticated communication with AltoCommand (AltoPlex devices only).
- Investigate issues and areas for optimization:
  - View incidents 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 on a map.
  - Use analytics to analyze long-term network behavior and link quality.
- Simplify common administrative tasks, such as:
  - Investigating details and generating log data for specific links or devices.
  - Link quality reporting.
  - Device configuration.
  - Fleet-wide device upgrades.
  - Network setup and device discovery.
  - Incident threshold configuration.
  - Intelligent rebeamforming activities (AltoPlex devices only).
  - Managing users / permissions.

AltoCommand supports:

- All AltoPlex devices. Must be at release 3.9.1 or later.
  - D621
  - D423
  - P621
  - P421

    - C420
    - C410
- Depending on the release level of your AltoCommand server, the server supports supports certain variants of earlier Gen2 Altowav devices.
    - Gen2 devices supported with AltoCommand release 4.x and newer:
        - K60 (both Hub and Remote roles). Must be at release 3.21 or later.
    - AltoCommand release 3.x and older:
        - K60
        - K60c
        - K60c+
        - K60i
        - K60x

  This guide covers AltoCommand release 4.x and newer. For information about AltoCommand release 3.x and older, see the AltoCommand Version 3.x User Guide.

Connect to the AltoCommand server

To connect to either the cloud-based or on-prem AltoCommand server:

1. In the address bar of a web browser, type the URL provided in the email you received from Altowav.
2. A warning message may indicate that the self-signed certificate used by AltoCommand is not recognized by the browser. Instructions to clear the message vary depending on the browser. For example, in Chrome:
    A. Click **Advanced**.
    B. Click **Proceed to...**
3. The AltoCommand server's web interface will open with the login dialog displayed:

    The default username is **admin**

    The default password is **admin**

After logging into the AltoCommand WebUI:

- If the instance of AltoCommand has not been given a name, or if no devices have been accepted on the server, the web interface will open to the **Settings** > **Site Devices** page.
    - For information about naming the AltoCommand instance, see Configure the name of the AltoCommand.
    - For information about accepting devices on the server, see Configure devices.
- Otherwise, the WebUI opens to the **Dashboard**.

Change the password for the admin user

Note: You are not required to change the password for the admin user, but it is strongly recommended.

To change password for the admin user, you must be logged in as a user with admin privileges.

1. Open the AltoCommand WebUI:

   In your browser's address bar, type:

   https://*hostname*

   where *hostname* is the fully qualified domain name of the AltoCommand server.

2. Log into the WebUI as a user with admin privileges.

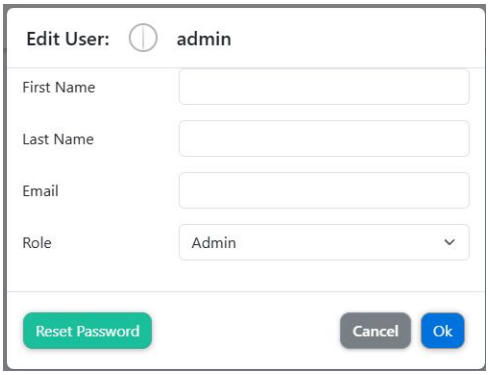
   The default username is **admin**

   The default password is **admin**

3. Click **Settings** > **Users**.

4. Click the **Edit** icon (✎) next to the admin user.

   The **Edit User** dialog opens.



5. Click **Reset Password**.
6. Type and confirm the new password and click **OK**.

   The password must be a minimum of eight characters and cannot start or end with whitespace characters.

You can also delete the admin user. Log in as another user with admin privileges and click the **Delete** icon (🗑) next to the admin user.

Note: Do not lose or forget the password of your admin user. The password cannot be reset.

Configure the name of the AltoCommand server

The first step in AltoCommand configuration is to give your instance of AltoCommand a name. Each instance of AltoCommand must have a name, both cloud-based and on-prem versions.

1. Open the AltoCommand WebUI:

   In your browser's address bar, type:

   https://*hostname*

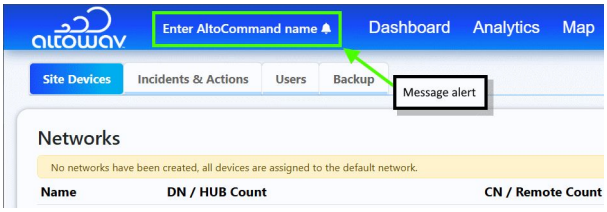
   where *hostname* is the fully qualified domain name of the AltoCommand server.

2. Log into the WebUI as a user with admin privileges.

   The default username is **admin**

   The default password is **admin**

   The WebUI will automatically open to the **Settings** > **Site Devices** page. A message alert in the Menu bar indicates that you need to configure the name of the AltoCommand server.



3. Click the message alert and type the name of the server.

   For example, this might be your corporate name, or the location that this instance of the AltoCommand will manage.

Networks

Networks in AltoCommand represent logical collections of devices, either based on physical location or other logical groupings such as all devices assigned to a specific customer. There can be multiple networks configured on a single instance of AltoCommand.

You can filter the information displayed in AltoCommand based on the selected Network. You can:

- View device information for one or more specific Networks.
- View all devices accepted on this instance of AltoCommand.
- View all devices that are not assigned to any Network. This is useful when new devices have been added, to determine which devices need to be assigned to Networks.

Create a Network

1. Open the AltoCommand WebUI:

   In your browser's address bar, type:

   https://*hostname*

   where *hostname* is the fully qualified domain name of the AltoCommand server.

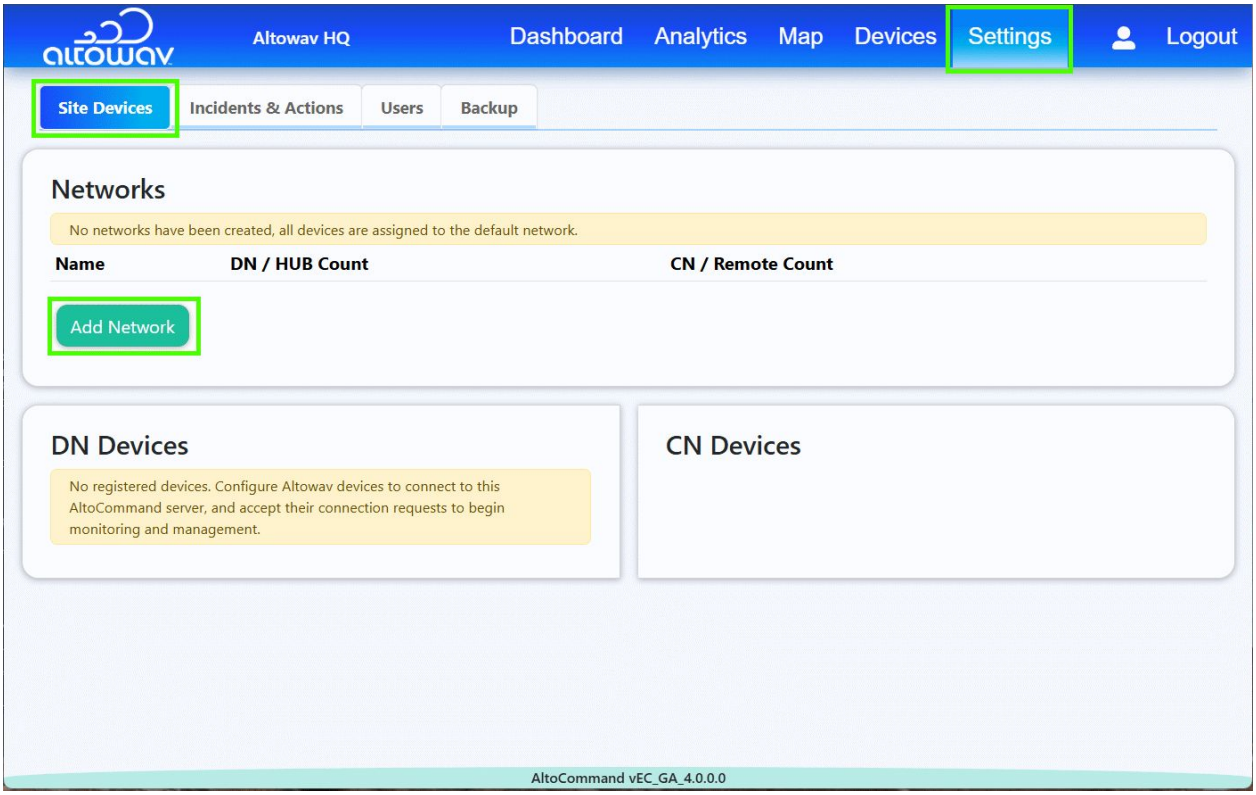
2. Log into the WebUI:

   The default username is **admin**

   The default password is **admin**

   - If devices have already been configured on the AltoCommand server, the WebUI will open to the **Dashboard**. In the menu bar, click **Settings** to advance to the **Site Devices** page.
   - If no devices have been configured, the WebUI will open to the **Settings** > **Site Devices** page.

3. Click **Add Network**.

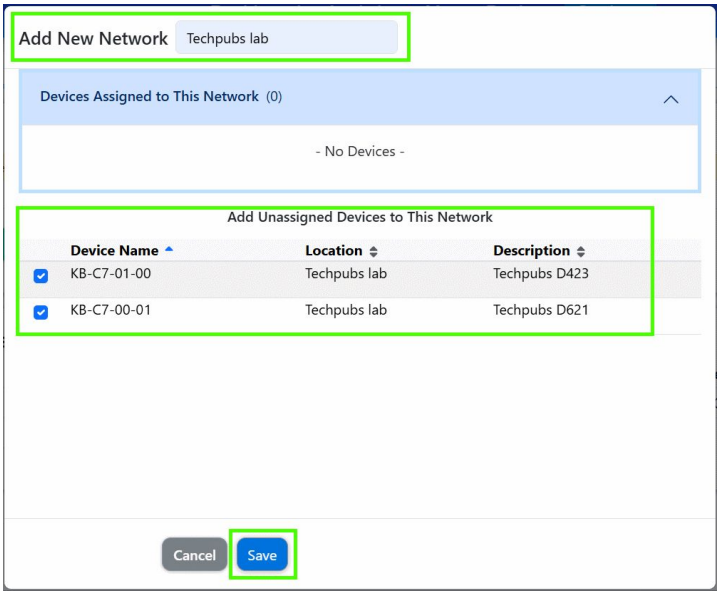


The **Add New Network** dialog opens.

4. For **Add New Network**, type the name of the network.
5. If there are unassigned devices available, select them as appropriate to add them to this network.

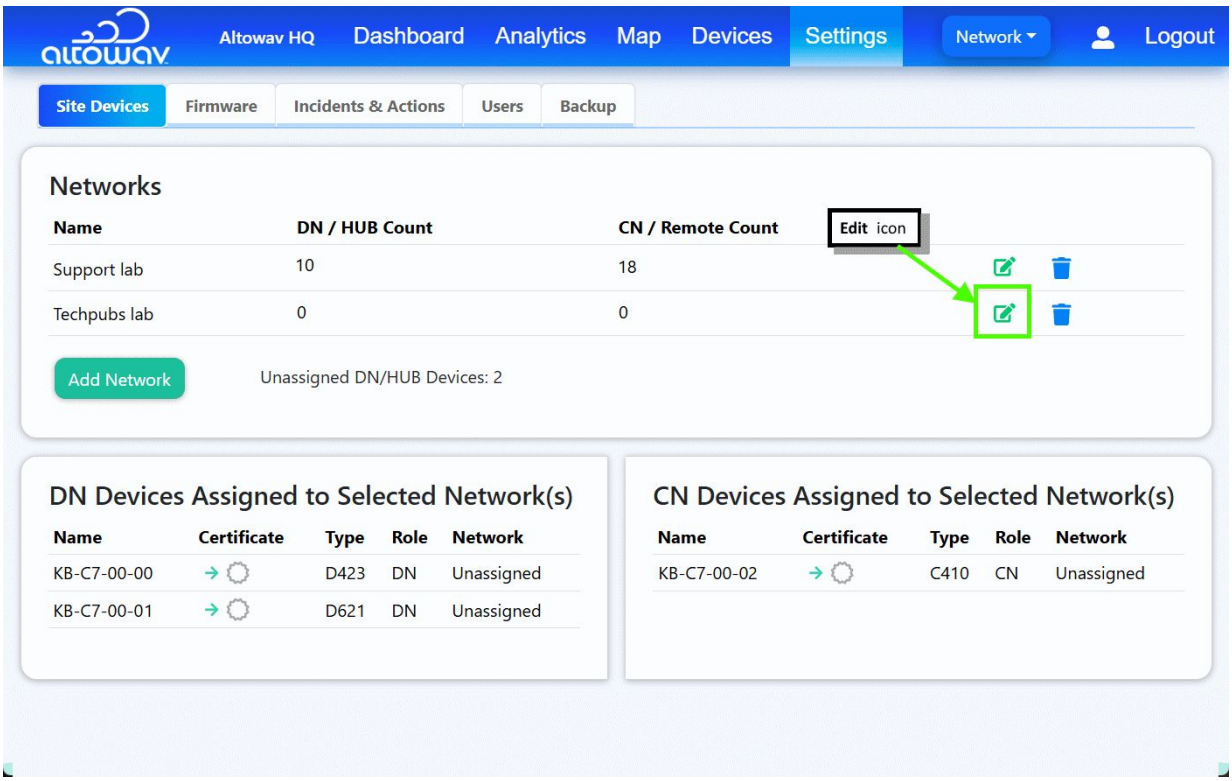
   Note: An unassigned device is a device that has been accepted on the AltoCommand server but has not been added to a network.

6. Click **Save**.

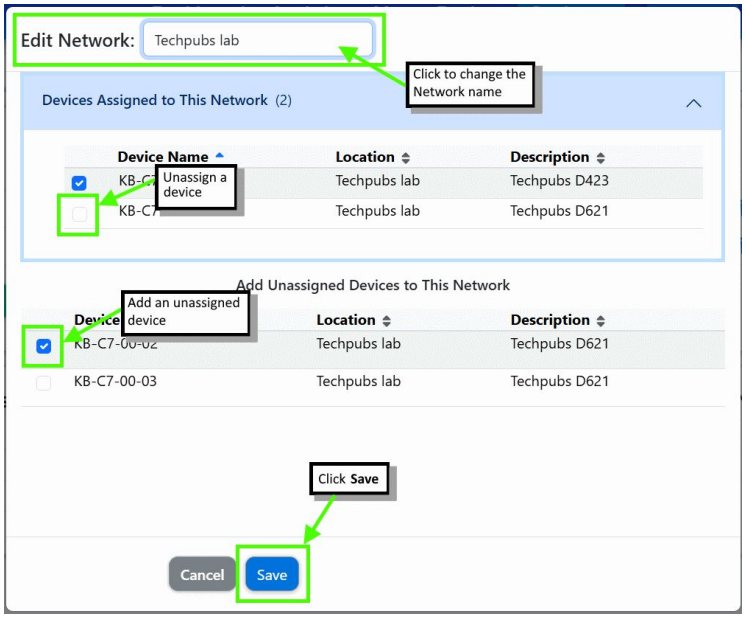


Edit an existing Network

To edit an existing Network, click the **Edit** icon (✎) next to the Network name.

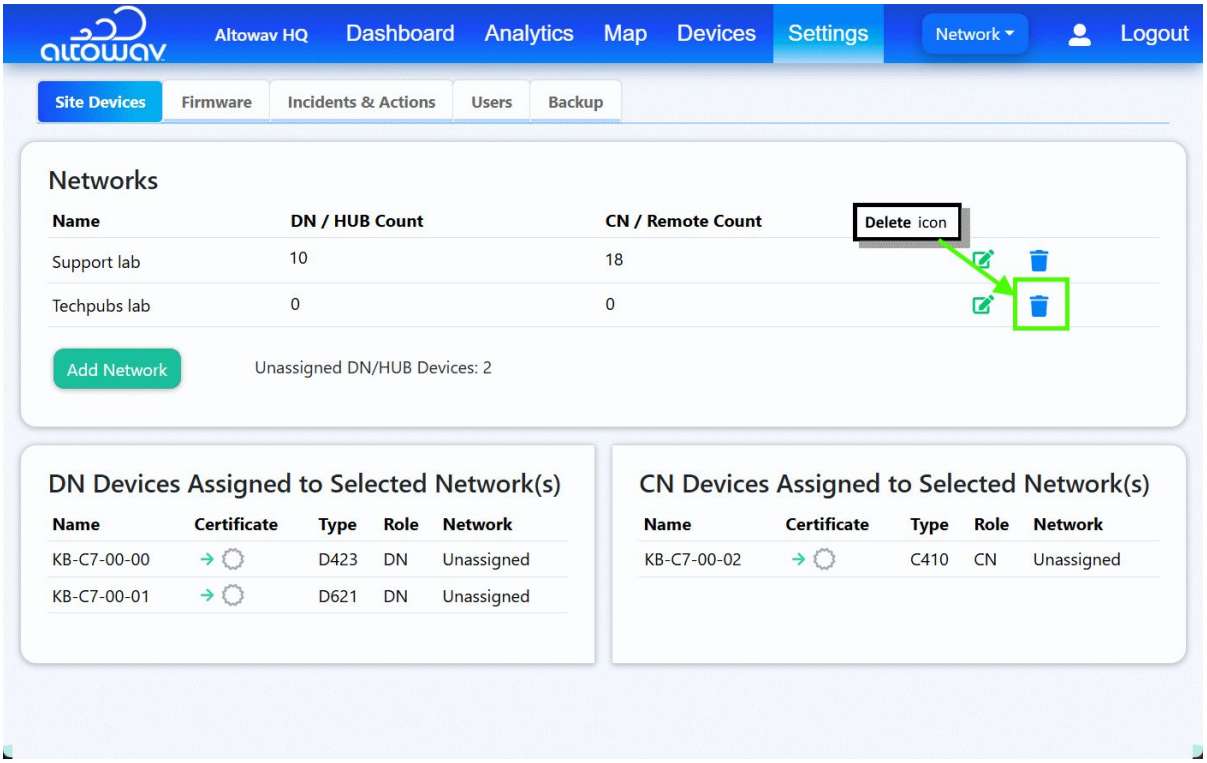


The **Edit Network** dialog opens. In this dialog, you can edit the name of the Network, unassign devices that have been assigned to the Network, and assign new devices. Click **Save** when done.



Delete a Network

To delete a Network, click the Delete icon (🗑) next to the Network name.



Note: You cannot delete a Network if it has devices assigned to it. First edit the Network to remove the devices, then delete the Network.

Assign devices to a Network

Devices can be assigned to a network at the same time that their connection request is accepted, as described in Accept connection requests from new devices. You can also assign devices to a Network after they have been accepted, and can remove devices from a Network and add them to another Network.

Only AltoPlex distribution nodes (DNs) and K60 hubs are added to Networks. Client nodes and remotes inherit the Network from the DN or hub they are connected to.

1. Open the AltoCommand WebUI:

   In your browser's address bar, type:

   https://*hostname*

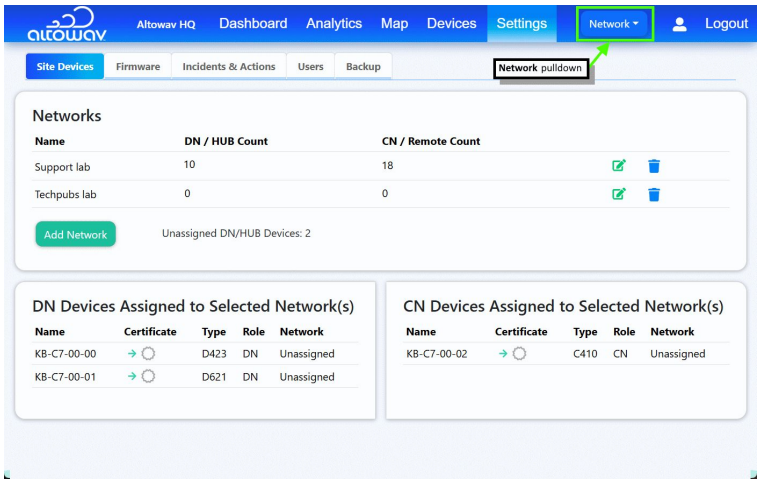
   where *hostname* is the fully qualified domain name of the AltoCommand server.

2. Log into the WebUI as a user with admin privileges.

   The default username is **admin**

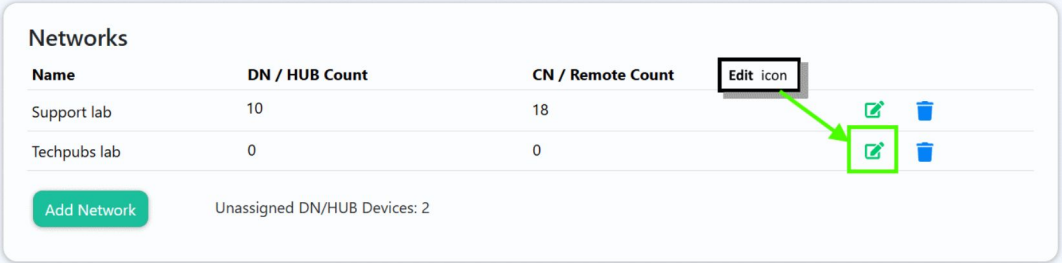
   The default password is **admin**

3. Click **Settings** > **Site Devices**.

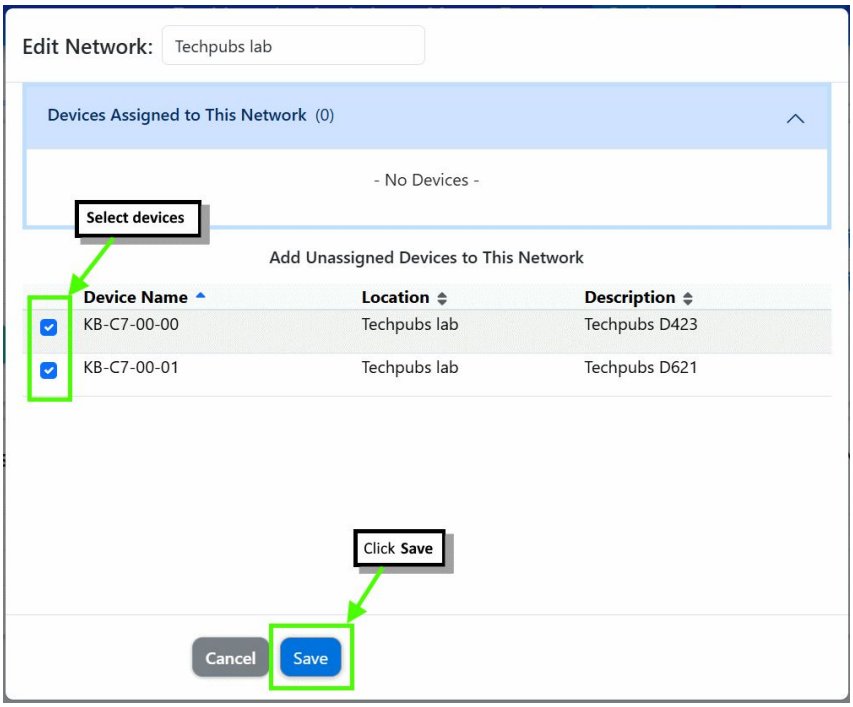


Note: In the **Site Devices** page, devices displayed in the **DN Devices Assigned to Selected Network(s)** and **CN Devices Assigned to Selected Network(s)** pane are filtered based on the selection in the **Network** pulldown. See Filter displayed information based on Networks for further information.

4. In the **Networks** pane, click the **Edit** icon ( ).



The **Edit Network** dialog opens.



5. Select unassigned devices that should be added to the Network and click **Save**.

   If the device you want to assign to the network is not available, it may be assigned to another network. Unassign it from that network first before attempting to assign it to this network.

Filter displayed information based on Networks

You can filter the information displayed in AltoCommand based on the selected Network. You can:

- View device information for one or more specific Networks.
- View all devices accepted on this instance of AltoCommand.
- View all devices that are not assigned to any Network. This is useful when new devices have been added, to determine which devices need to be assigned to Networks.

1. Open the AltoCommand WebUI:

   In your browser's address bar, type:

   https://*hostname*

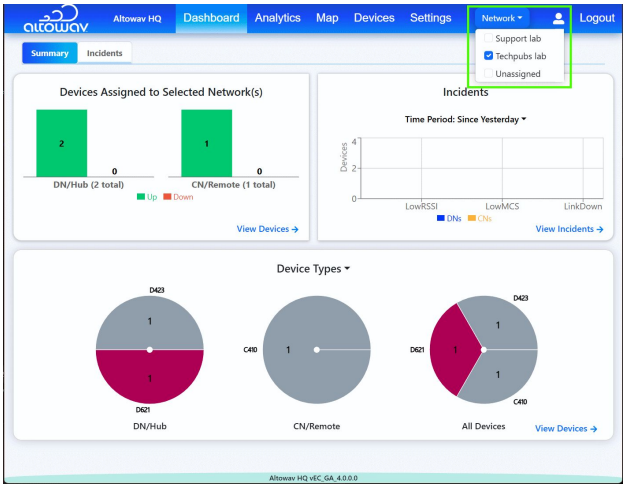
   where *hostname* is the fully qualified domain name of the AltoCommand server.

2. Log into the WebUI as a user with either user or admin privileges.

   The AltoCommand WebUI opens to the **Dashboard**.

   Information displayed in the **Dashboard** is filtered based on the Network selection. This is true for all windows in the WebUI until the Network selection is changed.

3. To change the Network selection, from the menu bar, click **Network** ▾ and select the appropriate Network or Networks.



Devices

Configure devices to connect to the AltoCommand server

With AltoCommand release 4.x and newer, the hostname or IP address of the AltoCommand server is set on the AltoPlex distribution node (DN) or point-to-point device, or on the the K60 radio. AltoPlex client nodes (CNs) inherit the AltoCommand server configuration from the DN to which they are linked.

Configure an AltoPlex or K60 device to connect to AltoCommand

Note: With AltoCommand 4.x and newer, AltoPlex devices must be at release 3.9.1 or newer. K60 radios must be at 3.21.230 or newer. Other Gen2 devices are not supported.

1. Log into the WebUI for an AltoPlex DN or point-to-point device, or for a K60 radio. See the device documentation for instructions.
2. In the WebUI for the device, click the **Admin** tab.
3. In the **Configuration** section, for **AltoCommand server**, type the fully-qualified domain name or IP address of the AltoCommand server.
4. Click **Save Changes**.

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

Note: After a device has been configured to request a connection to AltoCommand, it may take up to a minute for the device request to be displayed in the AltoCommand WebUI.

Accept connection requests from new devices

1. Open the AltoCommand WebUI:

   In your browser's address bar, type:

   https://*hostname*

   where *hostname* is the fully qualified domain name of the AltoCommand server.

2. Log into the WebUI as a user with admin privileges.

   The default username is **admin**

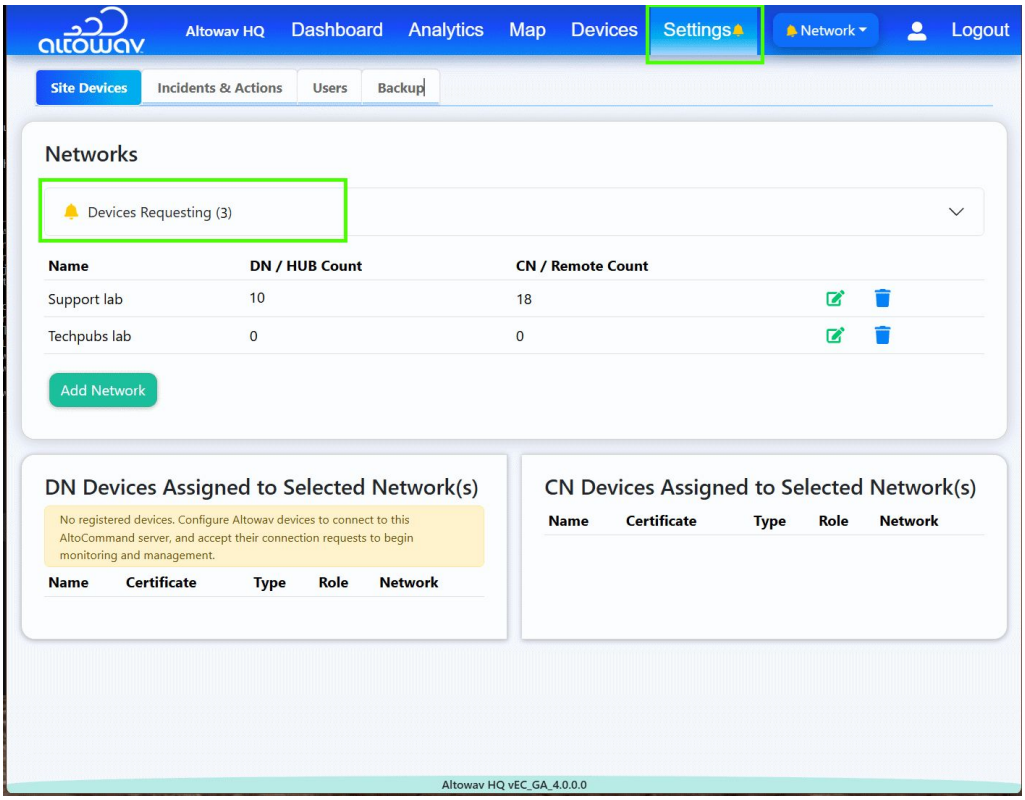
   The default password is **admin**

   Prior to any devices being accepted on the AltoCommand server, the WebUI will automatically open to the **Settings** > **Site Devices** page. Otherwise, click **Settings** 🔔 to open the **Settings** > **Site Devices** page.

   An **Alert** icon (🔔) next to **Settings** indicates that there are devices waiting to be approved.

   Note: After a device has been configured to request a connection to AltoCommand, it may take up to a minute for the device request to be displayed in the AltoCommand WebUI.



3. Click ⌄ next to 🔔 **Devices Requesting** to open the **Device Requesting** list.

Note: The number of devices allowed to connect to your instance of AltoCommand may be limited by your current licensing agreement. If so, you may receive a message similar to:

"License limit has been reached, additional devices connecting to AltoCommand will be refused. Please contact your Altowav sales representative."

4. Click **Accept** for each device.
5. Click **Save Changes**.

For AltoPlex devices, any connected CNs will be automatically added when the DN is added.

Assign devices to a Network

Devices can be assigned to a network at the same time that their connection request is accepted, as described in Accept connection requests from new devices. You can also assign devices to a Network after they have been accepted, and can remove devices from a Network and add them to another Network.

Only AltoPlex distribution nodes (DNs) and K60 hubs are added to Networks. Client nodes and remotes inherit the Network from the DN or hub they are connected to.

1. Open the AltoCommand WebUI:

   In your browser's address bar, type:

   https://*hostname*

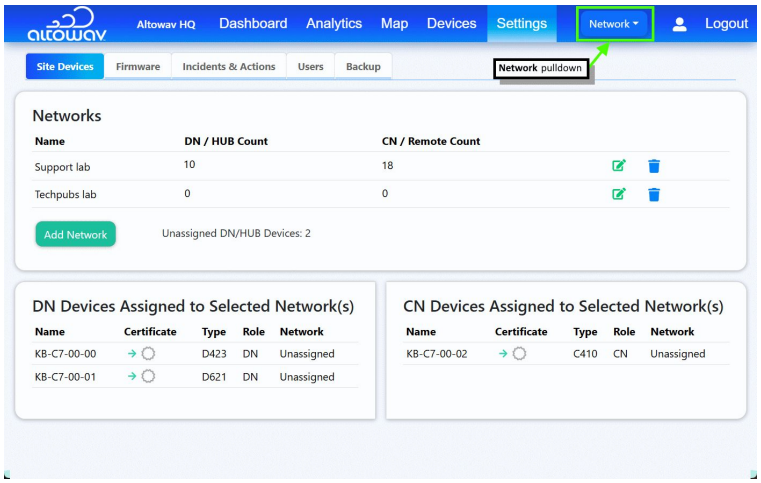
   where *hostname* is the fully qualified domain name of the AltoCommand server.

2. Log into the WebUI as a user with admin privileges.

   The default username is **admin**

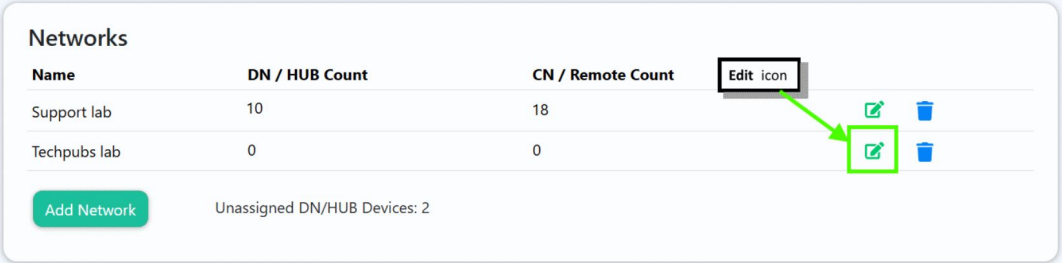
   The default password is **admin**

3. Click **Settings** > **Site Devices**.

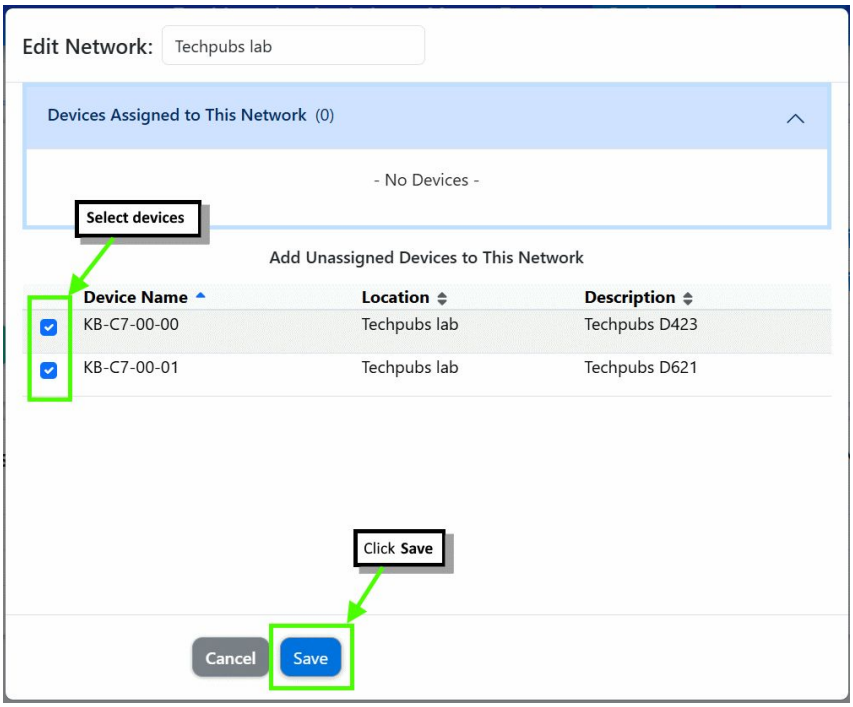


Note: In the **Site Devices** page, devices displayed in the **DN Devices Assigned to Selected Network(s)** and **CN Devices Assigned to Selected Network(s)** pane are filtered based on the selection in the **Network** pulldown. See Filter displayed information based on Networks for further information.

4. In the **Networks** pane, click the **Edit** icon ( ).



The **Edit Network** dialog opens.



5. Select unassigned devices that should be added to the Network and click **Save**.

   If the device you want to assign to the network is not available, it may be assigned to another network. Unassign it from that network first before attempting to assign it to this network.

Device authentication (AltoPlex devices only)

AltoCommand requires authenticated access to devices to be able to perform write operations to the device, including firmware upgrades and certain configuration tasks such as automated rebeamforming. To provide authenticated access, AltoCommand needs to install client certificates to have SSL-based authentication to AltoPlex devices.

To install a certificate on the device, AltoCommand requires write access to the device. If you have changed device's password, you will be asked to provide the password. The password is needed for one-time access to install the certificate, and is not stored on AltoCommand.

Note: For information about backing up AltoCommand certificates, see Back up and restore AltoCommand certificate files.

1. Open the AltoCommand WebUI:

   In your browser's address bar, type:

   https://*hostname*

   where *hostname* is the fully qualified domain name of the AltoCommand server.

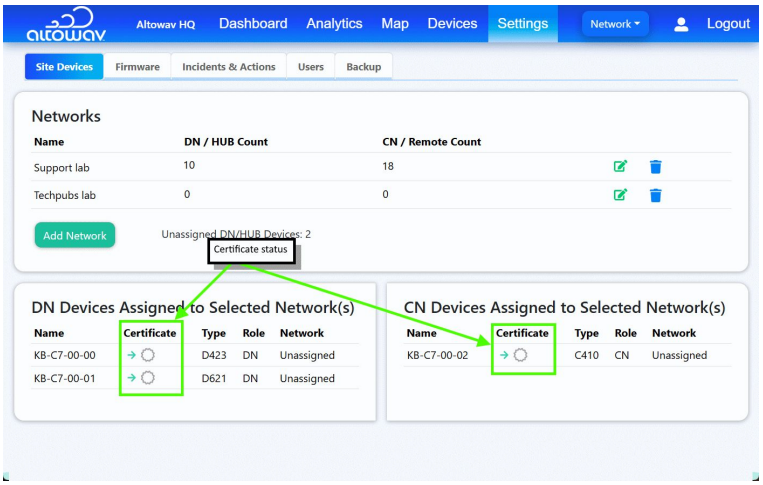
2. Log into the WebUI as a user with admin privileges.

   The default username is **admin**

   The default password is **admin**

3. Click **Settings** > **Site Devices**.
4. In the list of devices, under **Certificate**, an icon indicates the current certificate status.
5. For devices that have not yet been authenticated, click the icon in the **Certificate** column next to the device.

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



Certificate-related icons and remediation tasks

Various icons may appear in the **Certificate** column:

Icon	Meaning	Remediation
	Authentication is successful.	
	Authentication has not been performed.	Click the icon to begin the authentication process.
	Authentication failed.	Click the icon and select **Try again**.
	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.	Click the icon to reauthenticate on this instance of AltoCommand.

Delete an existing client certificate

Generally, it shouldn't be necessary to delete existing client certificates. For example, if a devices is moved from one instance of AltoCommand to another, simply click the **Reauthenticate** icon () to reauthenticate the device on the new instance of AltoCommand.

If you do need to delete the client certificate, do one of the following:

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

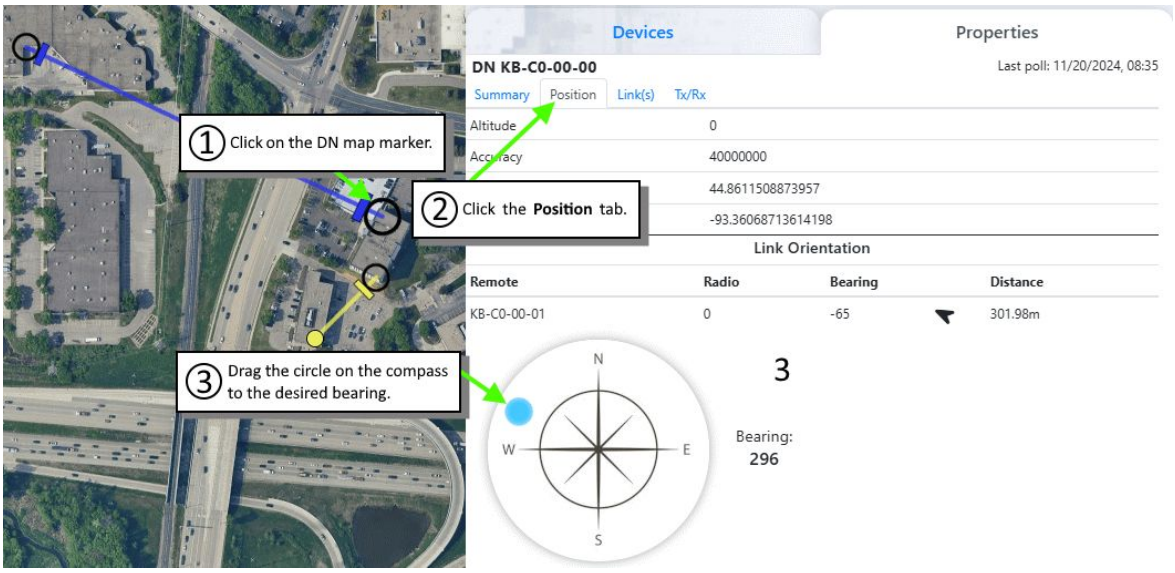
```
$ curl -k -u admin:admin \
https://server_name/rest/v002/security/install_client_ca_certificate?
reset=true \
-X POST \
-d ""
```

Where *server_name* is the IP address or hostname.local (KB-XX-XX-XX.local) of the device.

Adjust the position of devices on the Map

After devices have been added, you should adjust the position and bearing of the devices on the Map. This improves the accuracy of the Map for the purposes of planning, monitoring and optimizing the network.

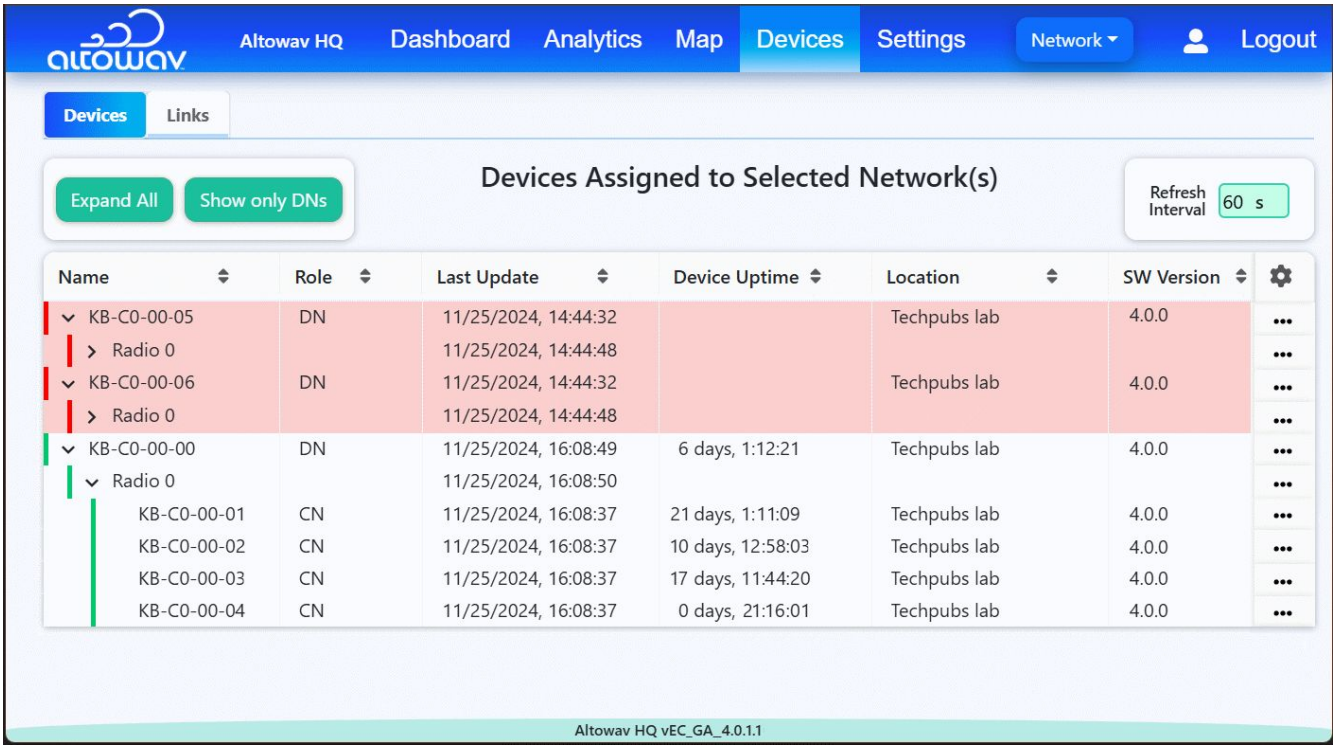
1. In the menu bar, click **Map**.
2. AltoPlex devices have GPS enabled by default, which allows the Map to automatically position them at or near their GPS location. For K60 devices, or AltoPlex devices with GPS disabled, drag the device from the tray to the correct location on the map.
3. Adjust the bearing (directional orientation) of the radio:
   A. Click the map marker for the radio.
   B. Click **Position**.
   C. Drag the circle on the compass to the desired bearing.



Devices page

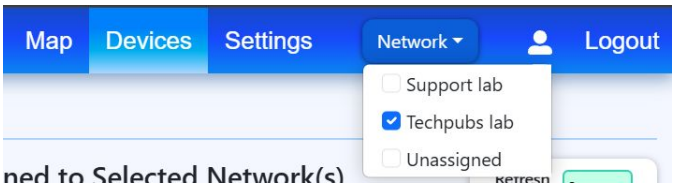
The **Devices** page shows a snapshot of device status, using color to highlight operational issues.

- 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 an issue with a link between devices.
- Light red highlighting on a row shows the device or sector with the broken links or reachability issue.
- Click › to expand or ⌄ to collapse the list of the device's interfaces and linked devices.



Sorting and filtering the Devices list

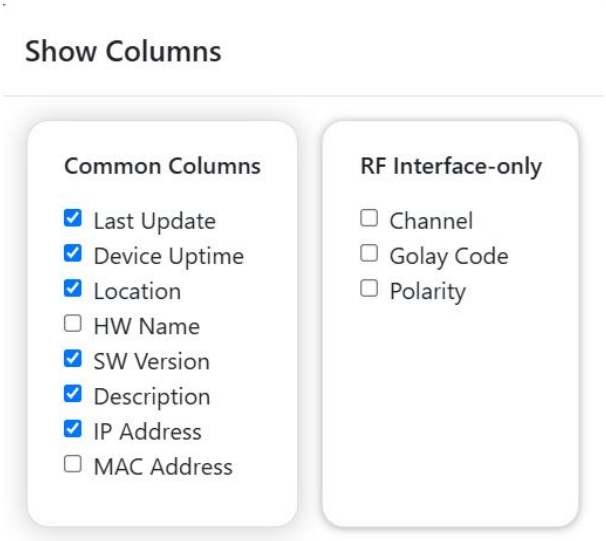
- To change the devices that are displayed based on the Network they are assigned to:
  1. In the menu bar, click **Network** ▾.



  2. Select the appropriate Network or Networks.
- Click a column heading to sort it by ascending (▲) or descending (▼) order.

- For any column, a **Filter** icon ( ) will appear when you hover the mouse over the column header. Click to open a menu allowing you to filter based on search criteria.

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



View device details

1. Open the AltoCommand WebUI:

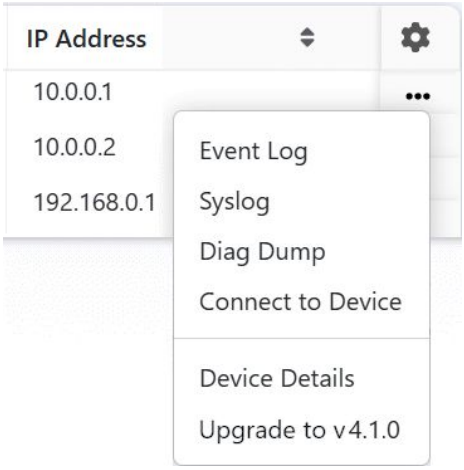
   In your browser's address bar, type:

   https://*hostname*

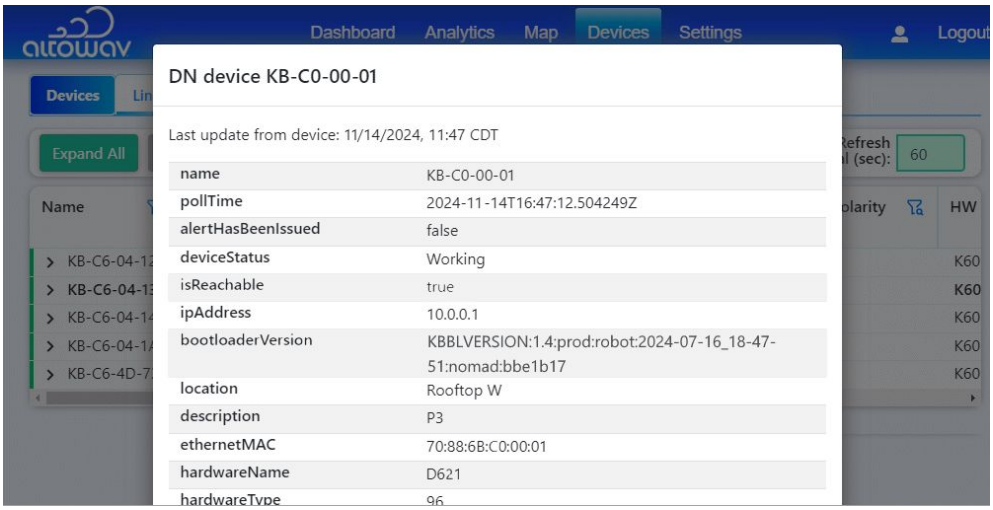
   where *hostname* is the fully qualified domain name of the AltoCommand server.

2. Log into the WebUI as a user with either user or admin privileges.

3. From the menu bar, click **Devices**.
4. Click the **Menu** icon (•••) at the end of the device's row.



5. Select **Device Details**.
6. The **Device Details** window opens, displaying detailed information about the device.



   Click anywhere outside of the **Device Details** window to close it.

Note: You can also click anywhere in the device's row to display the **Device Details** window.

Connect to a device

You can connect to an individual device's local WebUI from within AltoCommand:

1. Open the AltoCommand WebUI:

   In your browser's address bar, type:

   https://*hostname*

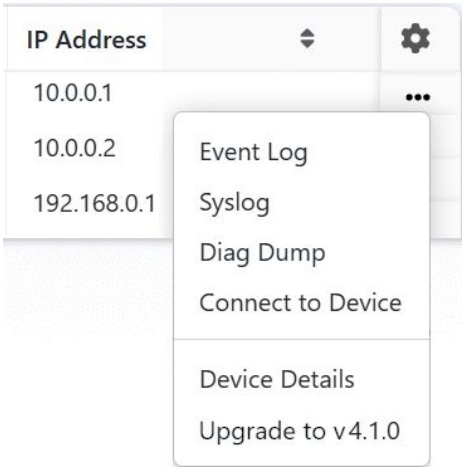
   where *hostname* is the fully qualified domain name of the AltoCommand server.

2. Log into the WebUI as a user with admin privileges.

   The default username is **admin**

   The default password is **admin**

3. From the menu bar, click **Devices**.
4. Click the **Menu** icon (•••) at the end of the device's row.



5. Click **Connect to Device**.

   The WebUI for the device will open in a new tab on your browser.

View device links

From the Devices page, you can view all links between devices, in a sortable table.

1. Open the AltoCommand WebUI:

   In your browser's address bar, type:

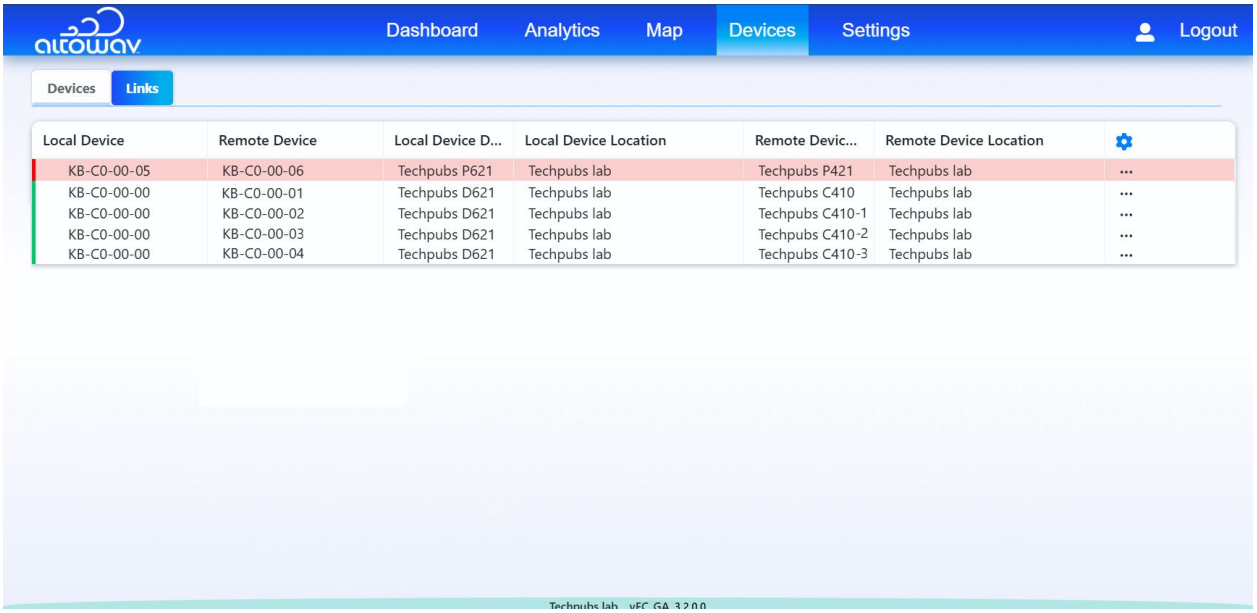
   https://*hostname*

   where *hostname* is the fully qualified domain name of the AltoCommand server.

2. Log into the WebUI as a user with either user or admin privileges.

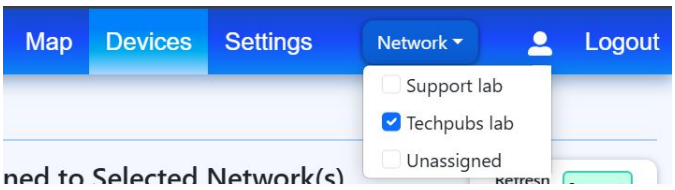
3. From the menu bar, click **Devices**.
4. Click the **Links** tab.

   The **Links** tab opens.



Sorting and filtering the Devices list

- To change the linked devices that are displayed based on the Network the devices are assigned to:
  1. In the menu bar, click **Network** ▾.



  2. Select the appropriate Network or Networks.
- Click a column heading to sort it by ascending (▲) or descending (▼) order.
- To select which columns to display, click the **Settings** icon (⚙).

View link details

1. Click the **Menu** icon (•••) at the end of the device's row.
2. Select **Link Details**.

   The **Link Details** window opens, displaying detailed information about the link.

   Click anywhere outside of the **Link Details** window to close it.

Note: You can also click anywhere in the link's row to display the **Link Details** window.

Manually reform a link between devices

It may be necessary to reform the link between two devices, if the current link is performing suboptimally. This process is known as rebeamforming. The recommended mechanism for rebeamforming is AltoCommand's intelligent rebeamforming, which will automatically sense when a link needs to be rebeamformed based on configurable parameters. Alternatively, you can manually reform the beam.

To manually rebeamform a link:

1. Open the AltoCommand WebUI:

   In your browser's address bar, type:

   https://*hostname*

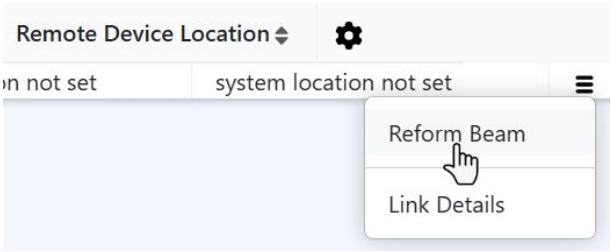
   where *hostname* is the fully qualified domain name of the AltoCommand server.

2. Log into the WebUI as a user with admin privileges.

   The default username is **admin**

   The default password is **admin**

3. From the menu bar, click **Devices**.
4. Click the **Links** tab.
5. Click the **Menu** icon (•••) at the end of the device's row.
6. Select **Reform Beam**.



View device logs

Two types of logs are available to view from the AltoCommand:

- **Event Log** — A subset of the system log, filtered for device events such as configuration changes, login attempts, and interface status changes.
- **Syslog** — The complete system log available from the device.

To view the device logs:

1. Open the AltoCommand WebUI:

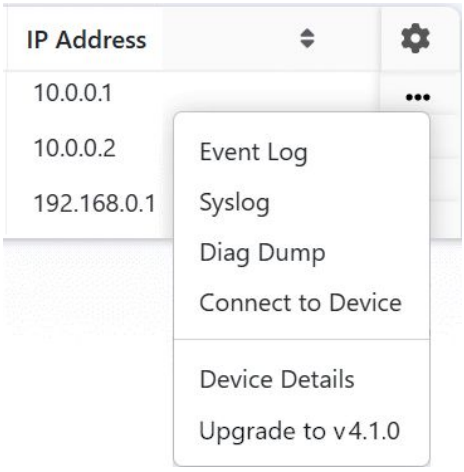
   In your browser's address bar, type:

   https://*hostname*

   where *hostname* is the fully qualified domain name of the AltoCommand server.

2. Log into the WebUI as a user with either user or admin privileges.

3. From the menu bar, click **Devices**.
4. Click the **Menu** icon (•••) at the end of the device's row.



5. Select either **Event Log** or **Syslog**.

   The log will open in a new browser tab.

Download a diagnostic file

A diagnostic file (also know as a diagnostic dump, or diag dump), provides a detailed log of all device activity, useful for Altowav support to investigate issues with a specific device.

To download a diagnostic file:

1. Open the AltoCommand WebUI:

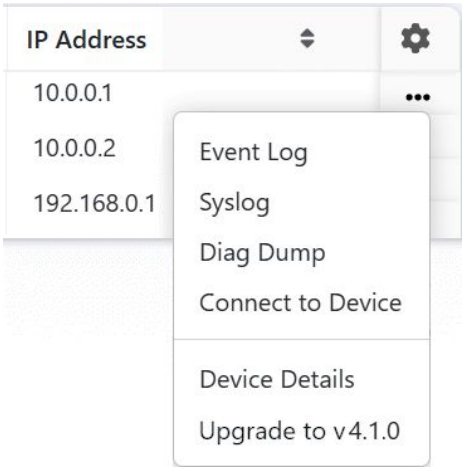
   In your browser's address bar, type:

   https://*hostname*

   where *hostname* is the fully qualified domain name of the AltoCommand server.

2. Log into the WebUI as a user with either user or admin privileges.

3. From the menu bar, click **Devices**.
4. Click the **Menu** icon (•••) at the end of the device's row.



5. Select **Diag Dump**.

   The diagnostic file will open in a new browser tab.

6. Click **Download** to download the file.

Upgrade the software on an individual device

The recommended method to upgrade device software is to perform a fleet upgrade. The fleet upgrade operations allows you to upgrade multiple devices with one click, and uses built-in AltoCommand intelligence to perform the upgrade in the proper sequence to minimize network downtime during device reboots and to insure that no device becomes unreachable during the process.

You can also perform device software upgrades on a case-by-case, individual basis.

Note: To use AltoCommand to upgrade an individual device, first upload the appropriate firmware file to AltoCommand and set the target firmware version.

1. Open the AltoCommand WebUI:

   In your browser's address bar, type:

   https://*hostname*

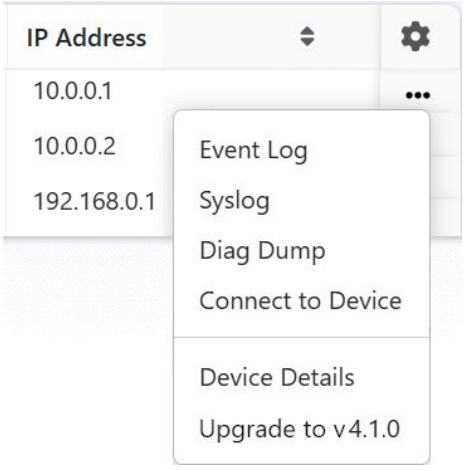
   where *hostname* is the fully qualified domain name of the AltoCommand server.

2. Log into the WebUI as a user with admin privileges.

   The default username is **admin**

   The default password is **admin**

3. From the menu bar, click **Devices**.
4. Click the **Menu** icon (•••) at the end of the device's row.



5. Select **Upgrade to *version***.

   The version listed here will correspond to the firmware version selected as the target version on the **Firmware** tab of the **Settings** page. See Set the target firmware version for more information.

The device will reboot as part of the upgrade process.

Remove devices from AltoCommand

Once a device have been configured to connect to AltoCommand, the device cannot be manual removed.

However, if:

- The device has been unreachable for ten days, and
- The device has no links to other devices connected to this instance of AltoCommand,

AltoCommand will purge the device from its database.

If a device is no longer active in the field, you should remove all links to that device from other devices. You can also unassign it from its network so that it will be listed in the unassigned network until it is purged. See device documentation for information about how to remove device links, and see Assign devices to a Network for information about device assignment.

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.

To open the **Dashboard**:

1. Open the AltoCommand WebUI:

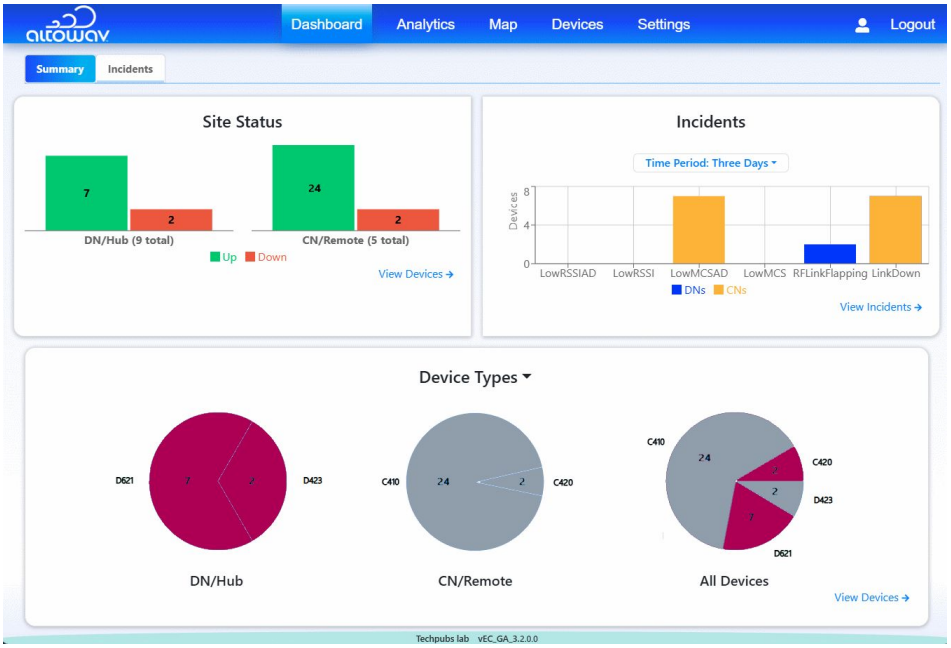
   In your browser's address bar, type:

   https://*hostname*

   where *hostname* is the fully qualified domain name of the AltoCommand server.

2. Log into the WebUI as a user with either user or admin privileges.

   The AltoCommand WebUI will open to the Dashboard's **Summary** page.

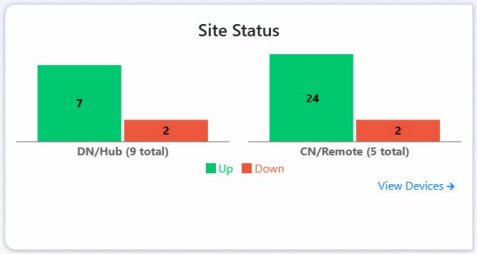


Links in each pane of the **Summary** page provide more detailed information about the reported status, incidents and software versions.

- 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**, **Software Versions**, and **Certificate Status**.

Site Status pane

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

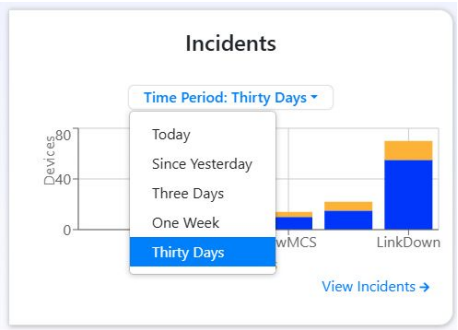


Click **View Devices** to go to the **Devices** page to investigate or resolve problems. The **Devices** page offers many filtering and viewing options, and links to each device's WebUI for configuration.

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

Incidents pane

The **Incidents** pane displays incidents by category from the selected amount of time.

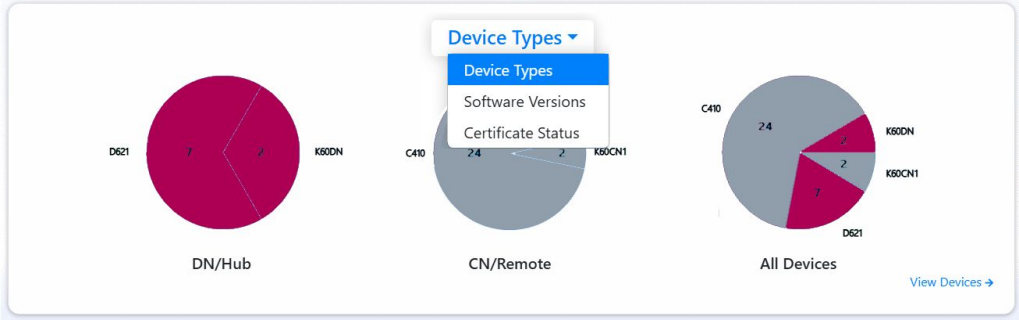


Click **View Incidents** to go to the **Incidents** tab to show more detail about specific incidents. See View information about incident reports for detailed information about the **Incidents** tab.

Thresholds for reported incidents can be set in the Incidents & Actions tab of the **Settings** page. See Configure incident reporting.

Device pane

The **Device** pane shows the device types.



- Select **Software Versions** to show the version of the software running on each device. See Fleet upgrade for further information.
- Select **Certificate Status** to show the status of the device's authentication with AltoCommand. See Device authentication for further information.
- Click **View Devices** to go to the **Devices** page.

View information about incident reports

The **Incident** pane of the the AltoCommand **Dashboard** provides a visual display of any reports of problems with your Altowav network, and the **Incidents** tab provides drill-down information about the incident reports.

To view information about incident reports:

1. Open the AltoCommand WebUI:

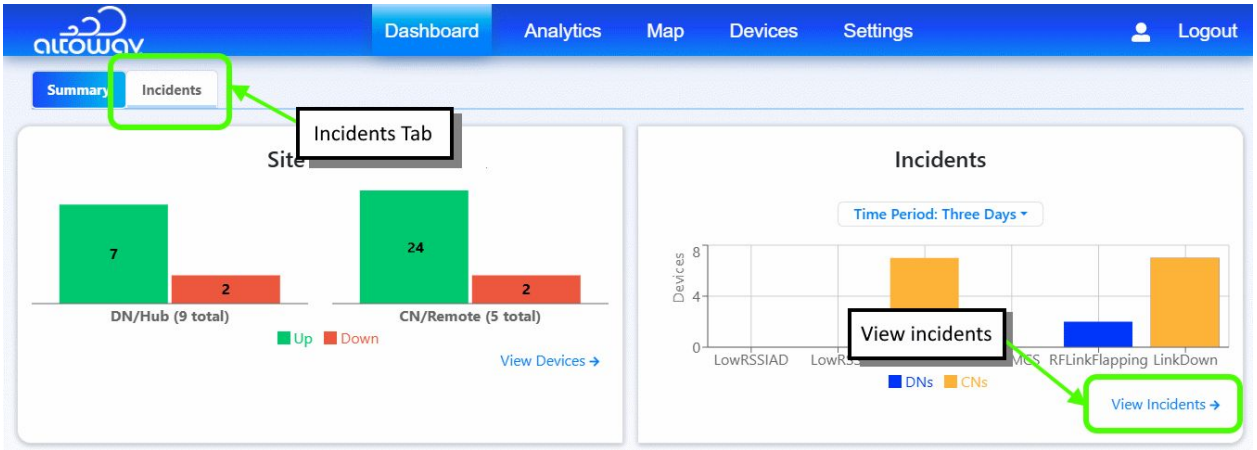
   In your browser's address bar, type:

   https://*hostname*

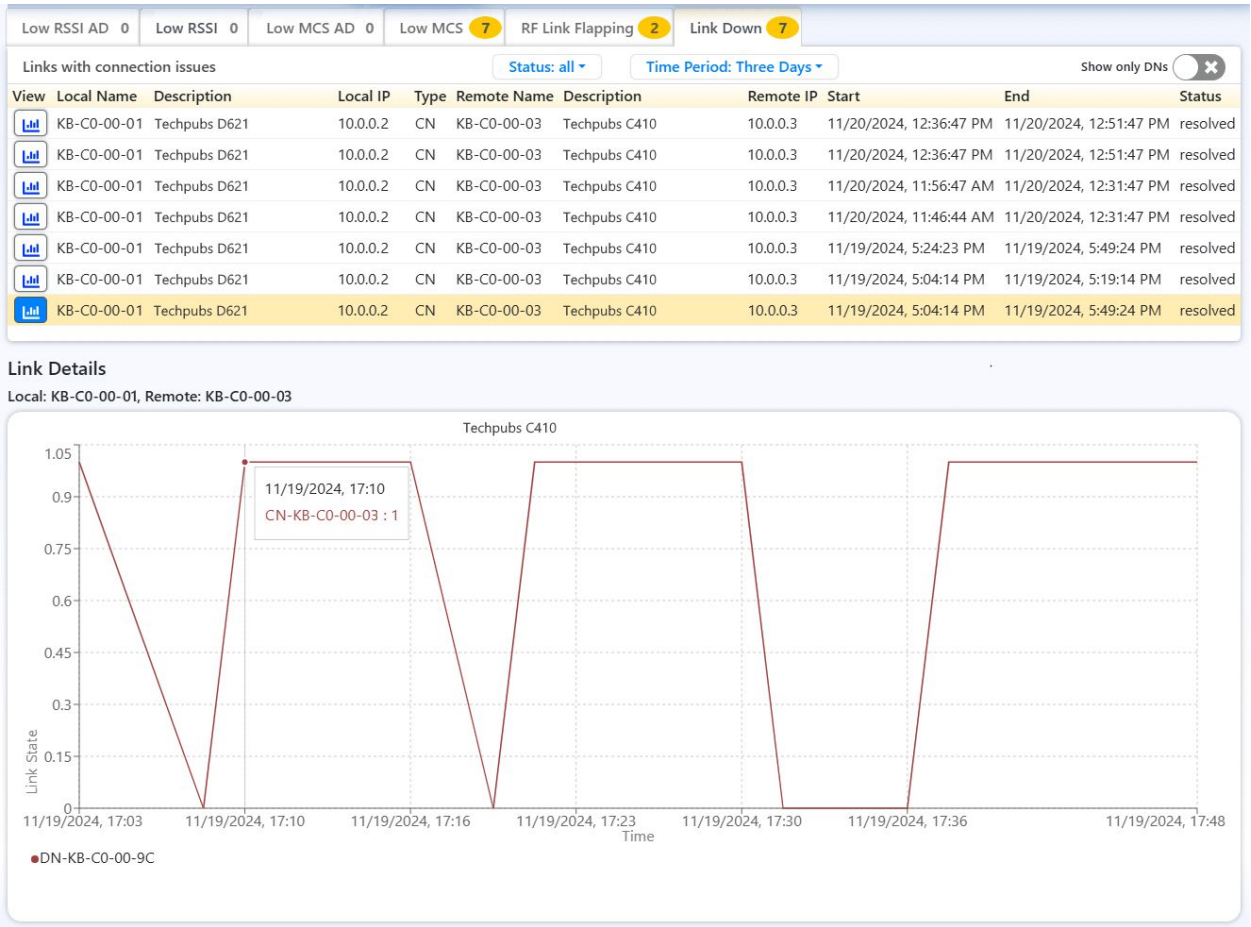
   where *hostname* is the fully qualified domain name of the AltoCommand server.

2. Log into the WebUI as a user with either user or admin privileges.

3. From the **Dashboard**, 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 K60 (802.11ad) devices.
- **Low RSSI** — Applies to AltoPlex (802.11ay) devices.

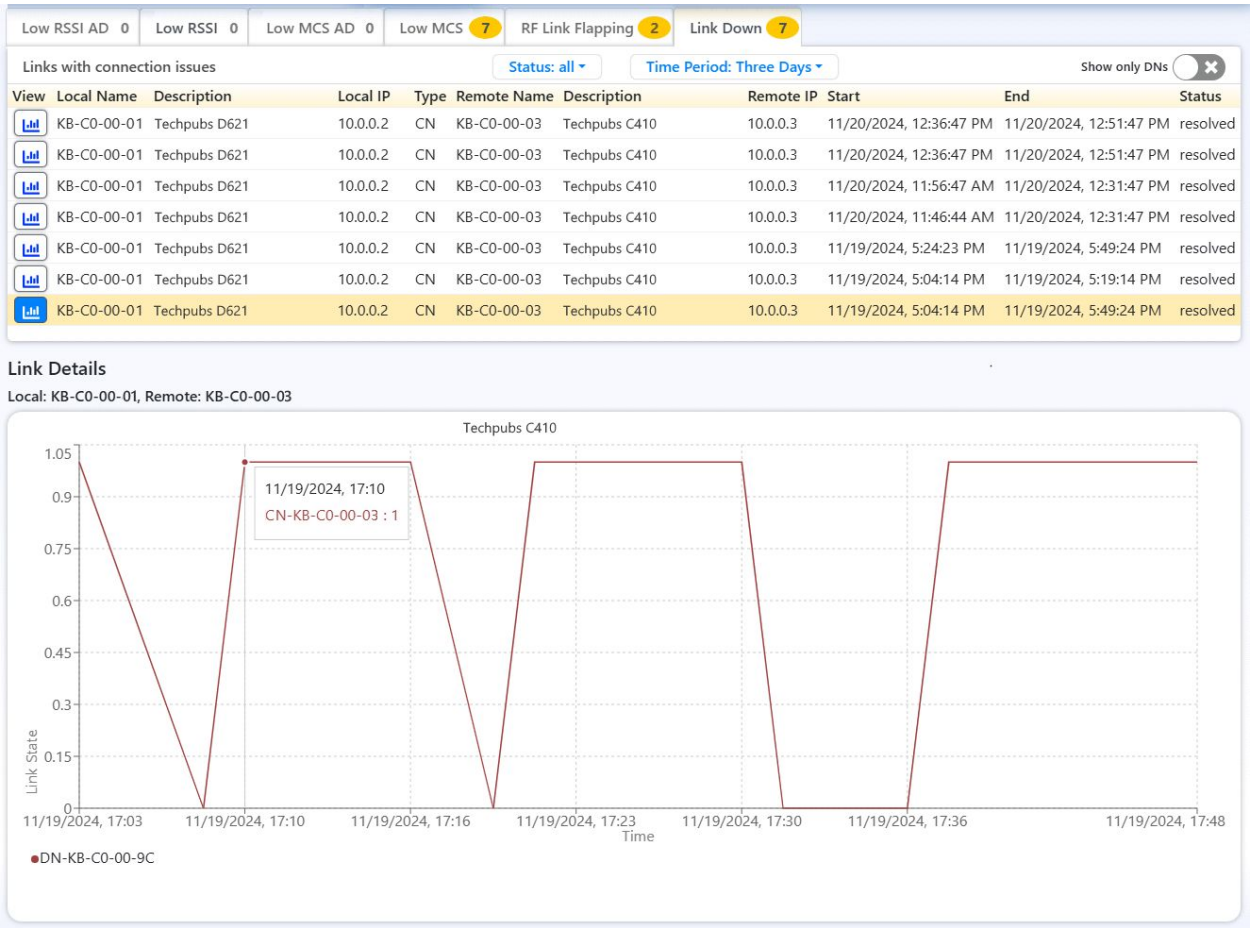
Low MCS — Lists reported incidents when the average weighted MCS level is less than the selected thresholds. Two tabs are available:

- **Low MCS AD** — Applies to K60 (802.11ad) devices.
- **Low MCS** — Applies to AltoPlex (802.11ay) devices.

RF Link Flapping - The RF link goes down and comes back up more than the configured threshold. (AltoPlex devices only.)

Link Down - Link is reported as down. (AltoPlex devices only.)

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



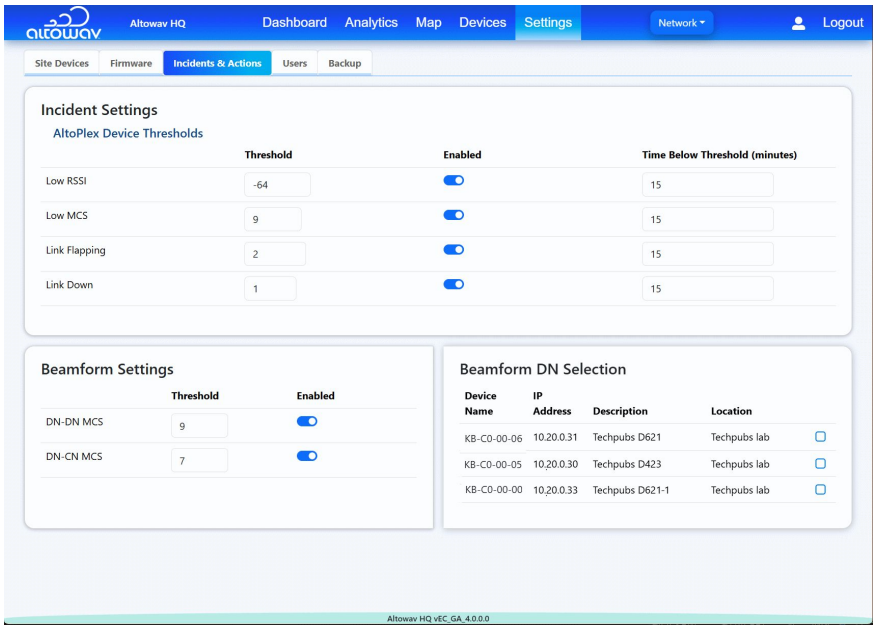
For further information about viewing incidents, see **Incidents** tab and Tips for viewing graphs.

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.

1. Click **Settings**.
2. Click **Settings** > **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**.

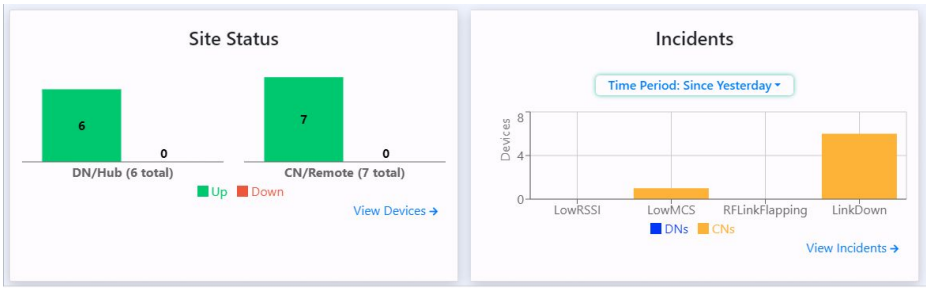
3. For each incident setting, set the appropriate threshold, enable/disable the incident report, and set the time.

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**.

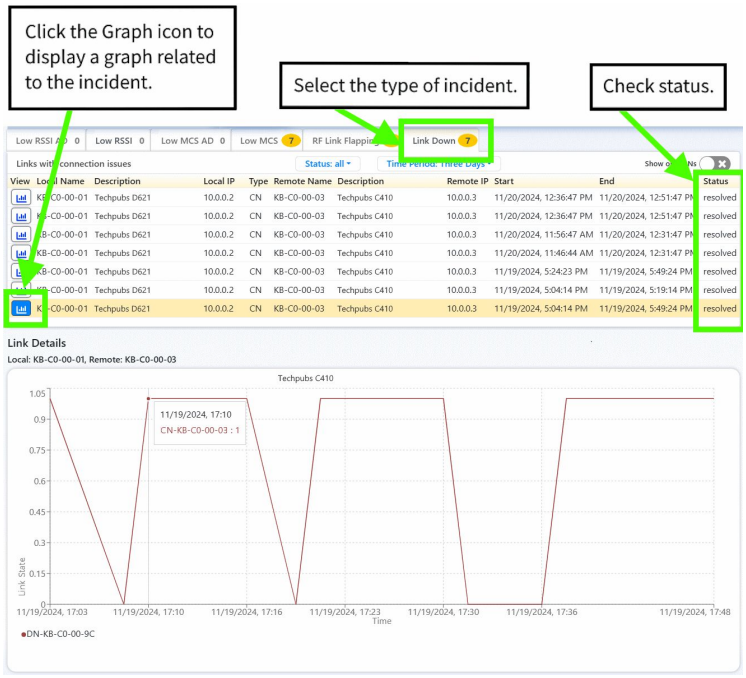


   - **Site Status** indicates that all links are currently up.
   - **Incidents** indicates that there were several links down in the last day.

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.

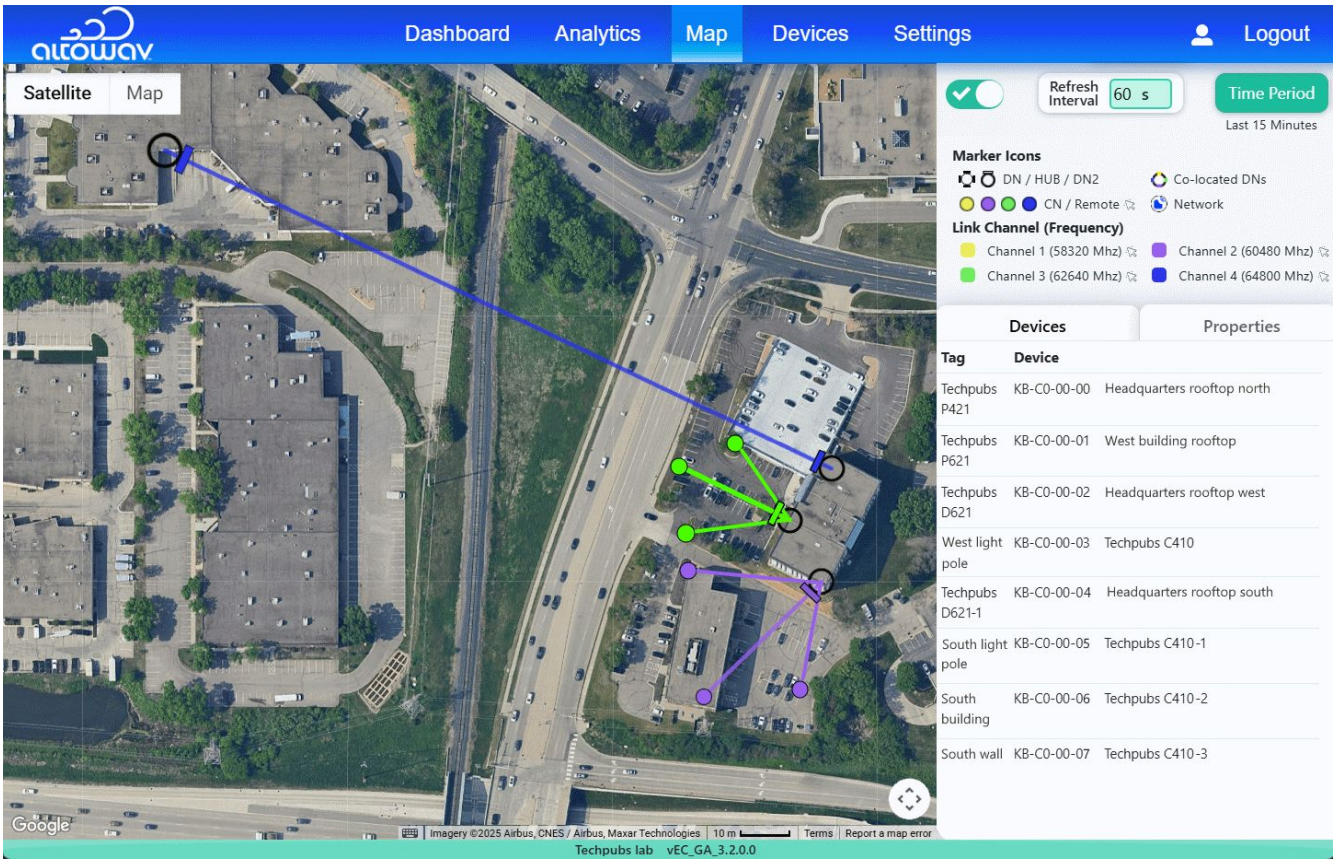


4. Hover at problematic areas on the graph such as a break or dip in the line, to determine the time of an incident.

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.

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.

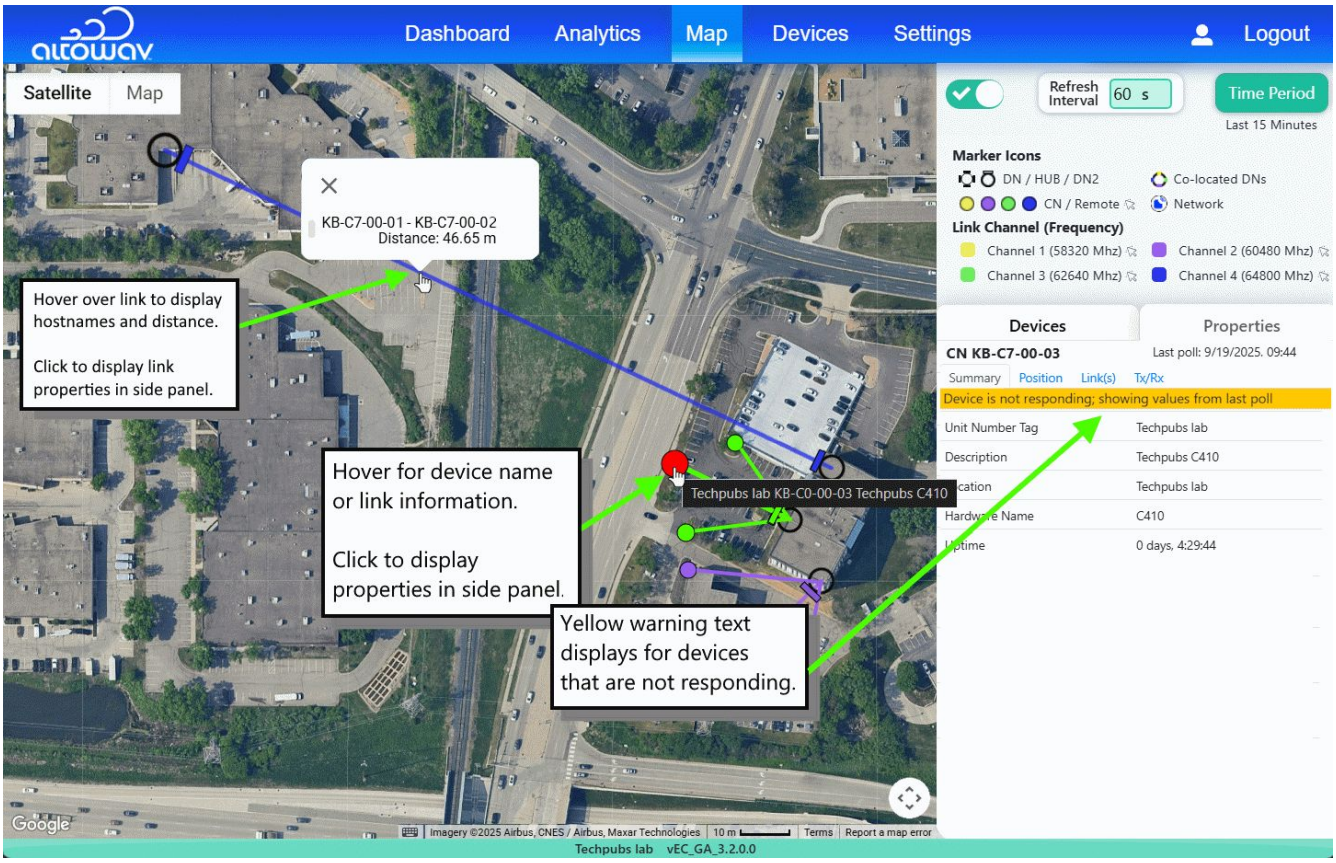


The Map key is at the top of the right sidebar, showing symbols for markers and colors used for each channel. You can hide the key by toggling off the **Key** toggle ( ). You can also set the **Refresh Interval** to configure how often AltoCommand refreshes data on the Map, and set the **Time Period** the configure the period of time that AltoCommand uses to compute average throughput. The **Pointer** icon ( ) next to a label indicates that clicking the label will toggle the category on and off.

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.

Hover over or click on a device or link to provide detailed information.

- Devices:
  - Hover over the device to display the hostname, location, and description.
  - The **Devices** tab in the sidebar lists all devices with with their tag and hostname. Click a device in the list or on the map to display a summary in the **Properties** tab.
- Links:
  - Hover over a link on the map to display the hostnames of the linked devices and the distance of the link, in meters.
  - Click the link to show one of the linked devices in the sidebar, with the **Link Properties** displayed. Click the link again to show the link properties from the other device.



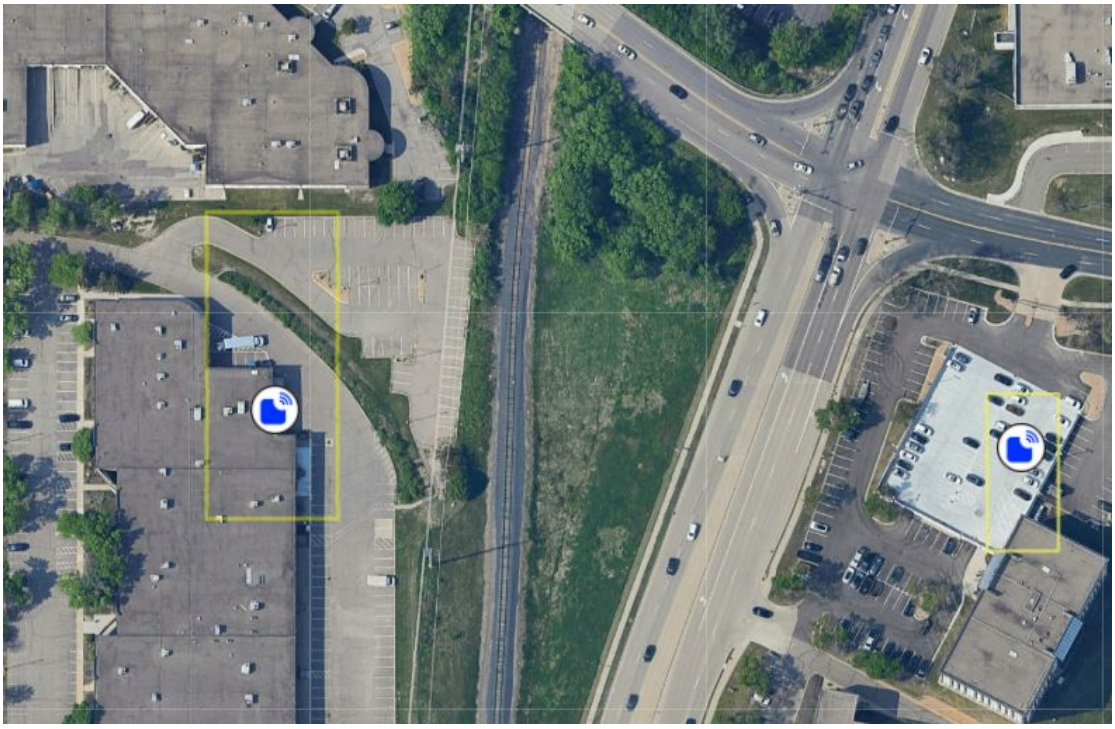
> **Tip:** Device GPS automatically positions DNs on the map, when available. (For Hubs or DNs without GPS enabled, the Map holds the device markers in a tray, until they are dragged to their accurate position.) Markers for connected CN and Remotes are positioned near their connected device. Adjust CN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

Using the Map with multiple Networks

When multiple Networks have been configured for your instance of AltoCommand, all Networks selected in the Networks pulldown are displayed on the Map. See Filter displayed information based on Networks for more information about displaying multiple Networks in AltoCommand.

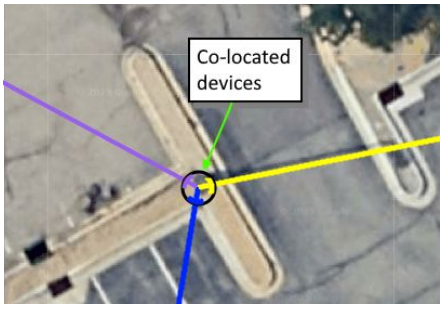
When multiple Networks are selected, the Map displays each network by using a **Network** icon ( ), and the geographical extent of each Network is indicated by a yellow bounding box.



Hover over the **Network** icon to see the Network name, and click a **Network** icon to give focus to that Network. The map will zoom into the geographical location of the Network with focus, and display its devices.

You can view the other networks by zooming out until you see their **Network** icon and yellow bounding box.

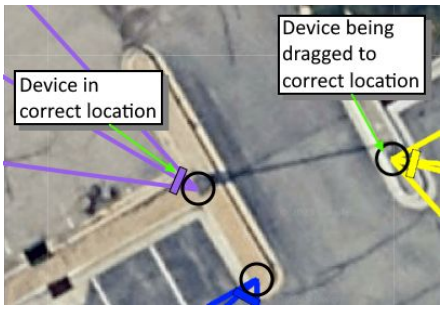
Co-located devices



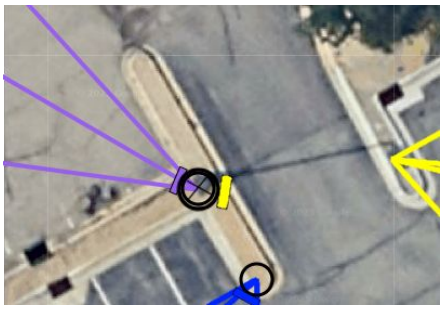
Devices that are installed close to each other (for example, on the same pole) are considered co-located devices. When possible, AltoCommand will use GPS positioning information to display co-located devices as joined together on the same marker.

Because of the imprecision of GPS data, some co-located devices may be indicated on the Map as near each other, but not co-located. You can drag the devices to their correct location and join them together to indicate on the map that they are co-located:

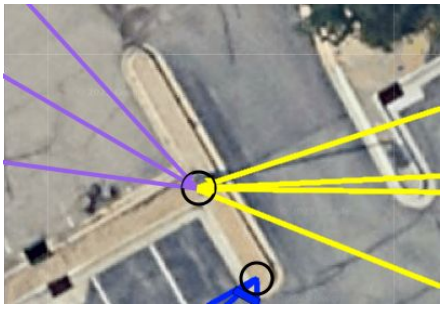
1. If the first device is not in the correct location, drag the device to the correct location.
2. Click on the second device and begin dragging it. An x will appear inside the device marker.



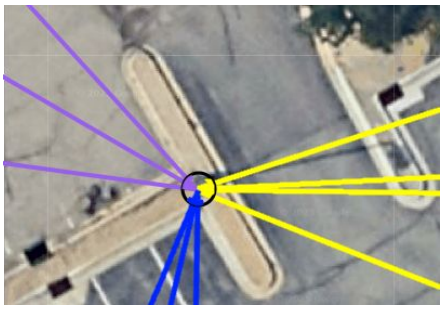
3. Drag the incorrectly-located device on top of the black marker for the correct device.



4. Drop the device into place.

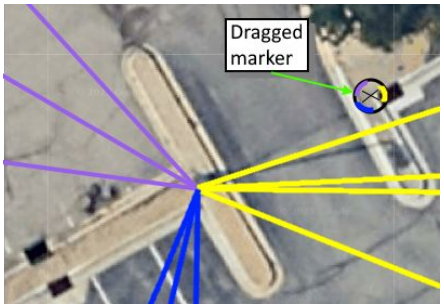


5. Repeat for any other co-located devices.

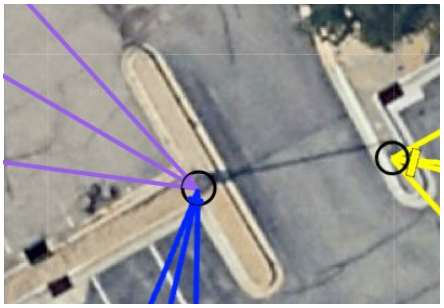


Another possibility is that AltoCommand may incorrectly determine that two or more devices are co-located, when they are in fact near to each other but in different locations. To rectify this situation:

1. Click on the marker for the co-located devices and drag to an alternate location.



2. Drop the device marker. This will place one of the devices in the new location, and will return the other devices to the original (co-located) location.

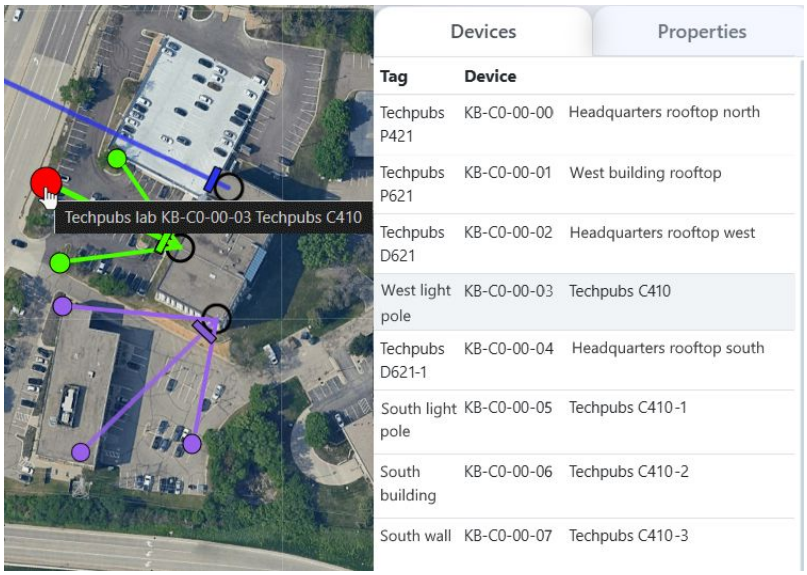


The Map side panel

The Map side panel, displayed to the right of the map, displays a map key, configurable refresh interval and time period for computing average throughput, and device information.

Devices tab on the side panel

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.

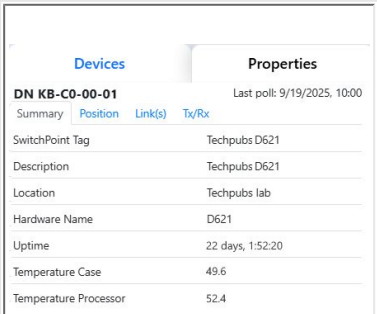
See the device documentation for information about how to configure the description and location.

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

Properties tab on map side panel

Click on a device in the list or on the Map to show its **Properties**. For co-located devices, clicking on the co-location marker on the Map will sequence through each co-located device and display that device's **Properties**.

The **Properties** tab has four sub-tabs — **Summary**, **Position**, **Link(s)** and **TX/RX throughput**:

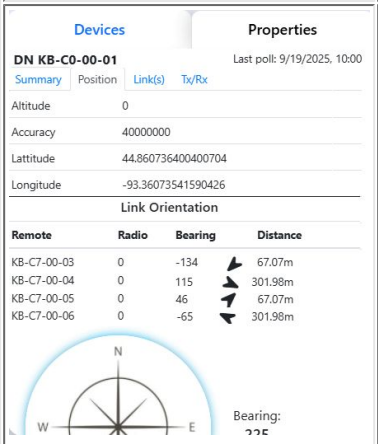


Summary

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



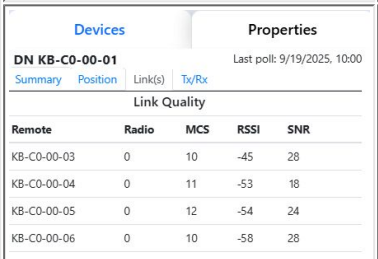
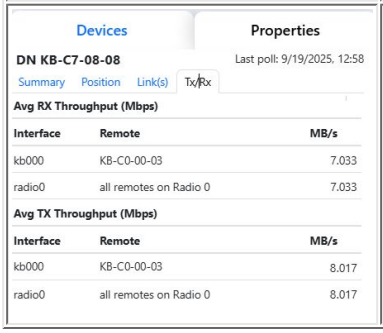
Position

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

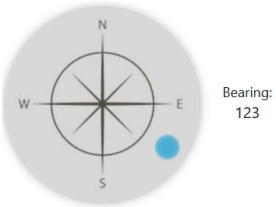
Link Orientation information is bearing and distance information taken from the map. Drag the marker to the actual location. Links listed are from the K60's configuration.

	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, including the radio interface, MCS, RSSI and SNR for each link. Click on a link to show the attributes of the linked device. **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. This represents the average throughput during the most recent time period, as configured by using the **Time Period** button at the top of the side bar.

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 CNs or Remotes are added to the map near the DN or Hub to which they connect. Drag the CN markers to their actual installed location on the map.

Client nodes at initial location on the Map.

Client nodes moved to their correct location on the Map.

Review a network by using the Map

To view the Map:

1. Open the AltoCommand WebUI:

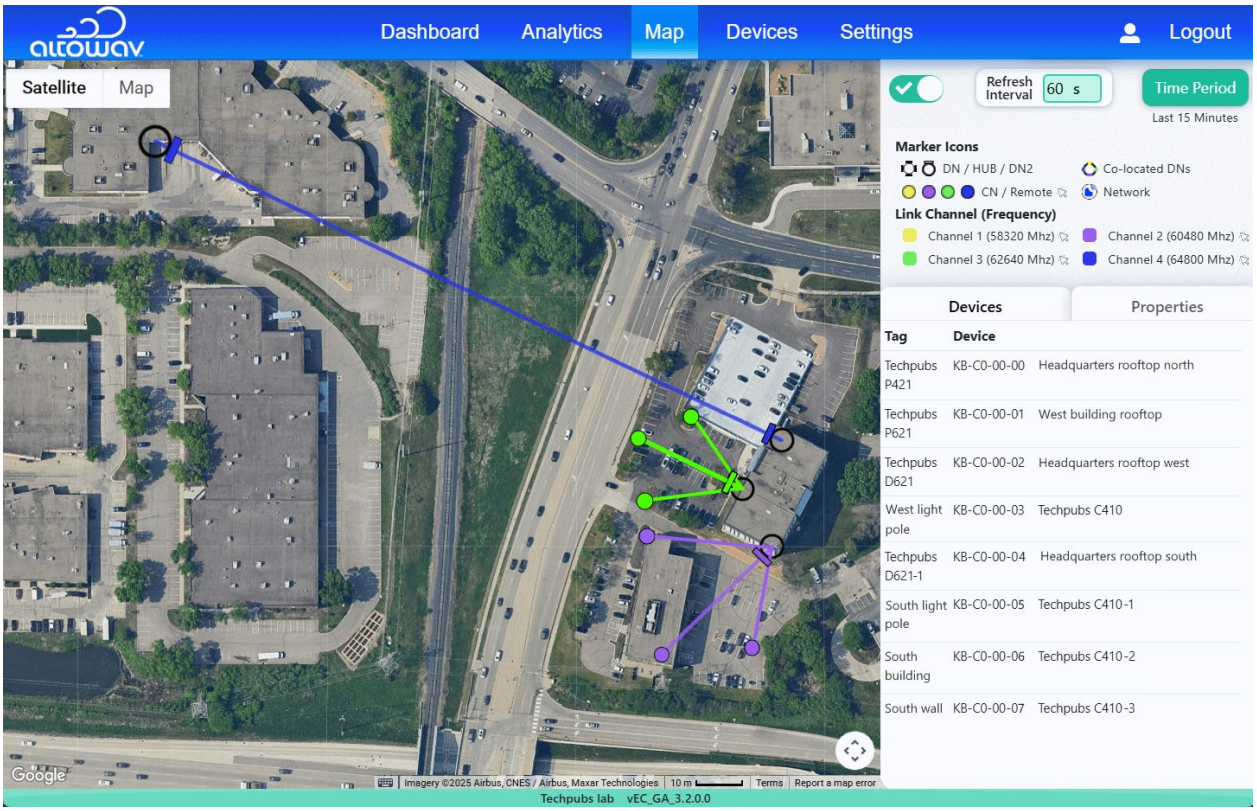
   In your browser's address bar, type:

   https://*hostname*

   where *hostname* is the fully qualified domain name of the AltoCommand server.

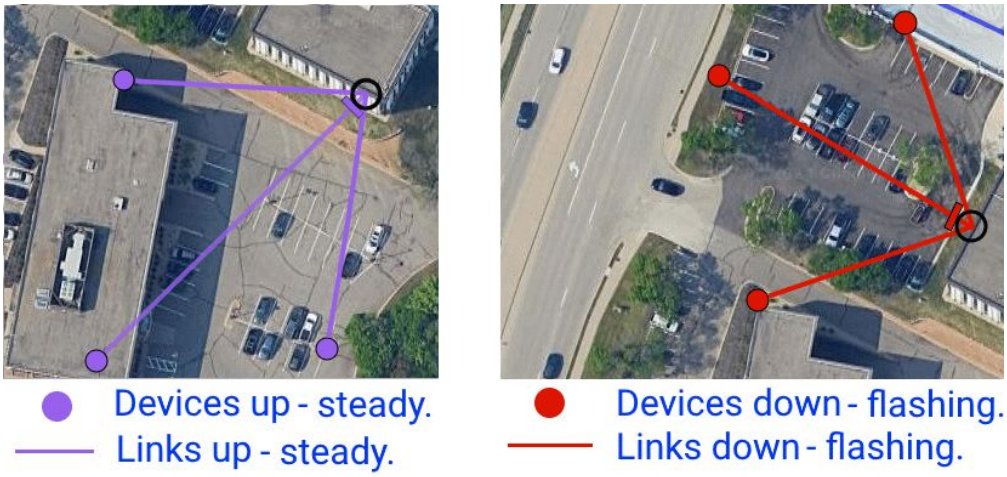
2. Log into the WebUI as a user with either user or admin privileges.

3. From the menu bar, click **Map**.



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.

Monitoring and optimizing tasks

The following are various monitoring and optimizing tasks available from within AltoCommand:

- View the **Dashboard** for a quick assessment of the status of your network's health, including devices that are down, and incident reports.
- Investigate incident reports, including:
  - Configure incident reporting.
  - Example: How to investigate reported incidents of links down, when all devices are up.
- Review a network on the Map.
- Use AltoCommand to refine network performance.
- Enable intelligent rebeamforming.

Analytics

The **Analytics** 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.

To view the **Analytics** page:

1. Open the AltoCommand WebUI:

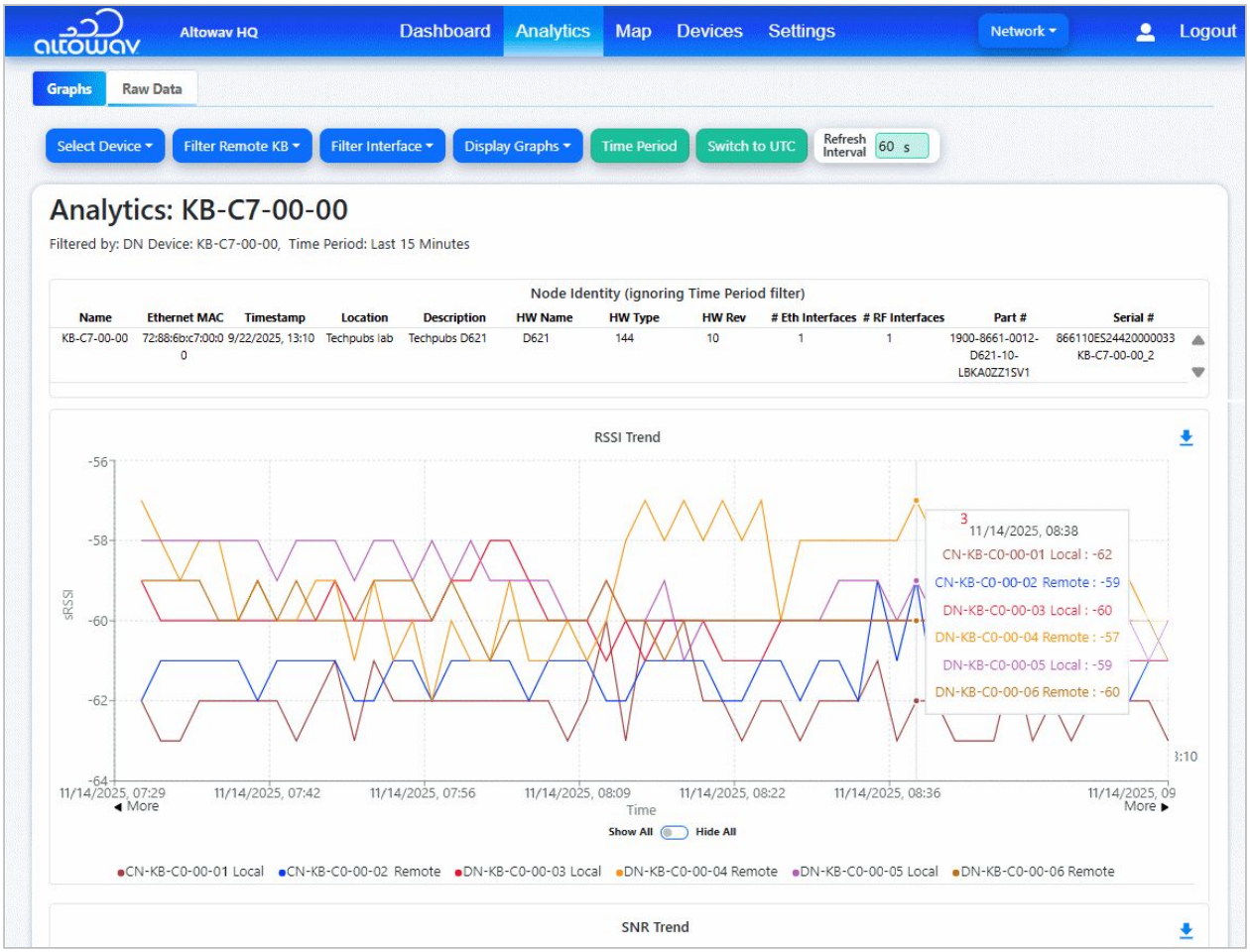
   In your browser's address bar, type:

   https://*hostname*

   where *hostname* is the fully qualified domain name of the AltoCommand server.

2. Log into the WebUI as a user with either user or admin privileges.
3. From the menu bar, click **Analytics**.

   The **Analytics** page opens.



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-C0-00-00_Thu, 26 Oct 2025 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 allows you to filter 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.

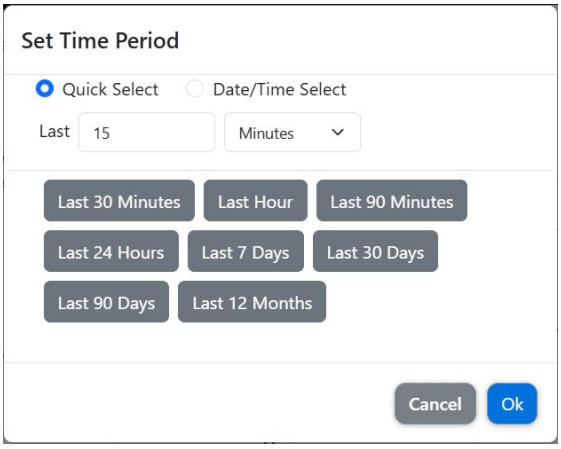
Filter Interface — Select the specific interface(s) on the selected device to graph. This is useful for devices with multiple interfaces, such as the K60DN. Default: **Select all**.

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.
- **Link Quality** (K60 only) — A number between 0 and 100 indicating the quality of the link.
- **sSNREst** (AltoPlex only) — Graphs signal to noise ratio estimate.
- **TX Power Index** (AltoPlex only) — Graphs the transmission power in dBm as polled from devices at the local and remote ends of the link. (AltoPlex devices only.)
- **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.
- **Rx Beam Azimuth** (AltoPlex only) — The Rx beam angle. (AltoPlex devices only.)
- **Tx Beam Azimuth** (AltoPlex only) — The Tx beam angle. (AltoPlex devices only.)
- **Throughput** — Displays transmission and receiving performance for the link measured in Mb/sec.
- **Block Error Rate (nSyn/nCW)** (AltoPlex only) — Displays a ratio of erroneous blocks to the total blocks transmitted. (AltoPlex devices only.)
- **Device Temperature** — The temperature of the device over time.
- **GPS Accuracy** (AltoPlex only) — The accuracy of the latest reading, in meters, of the device's GPS.

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.

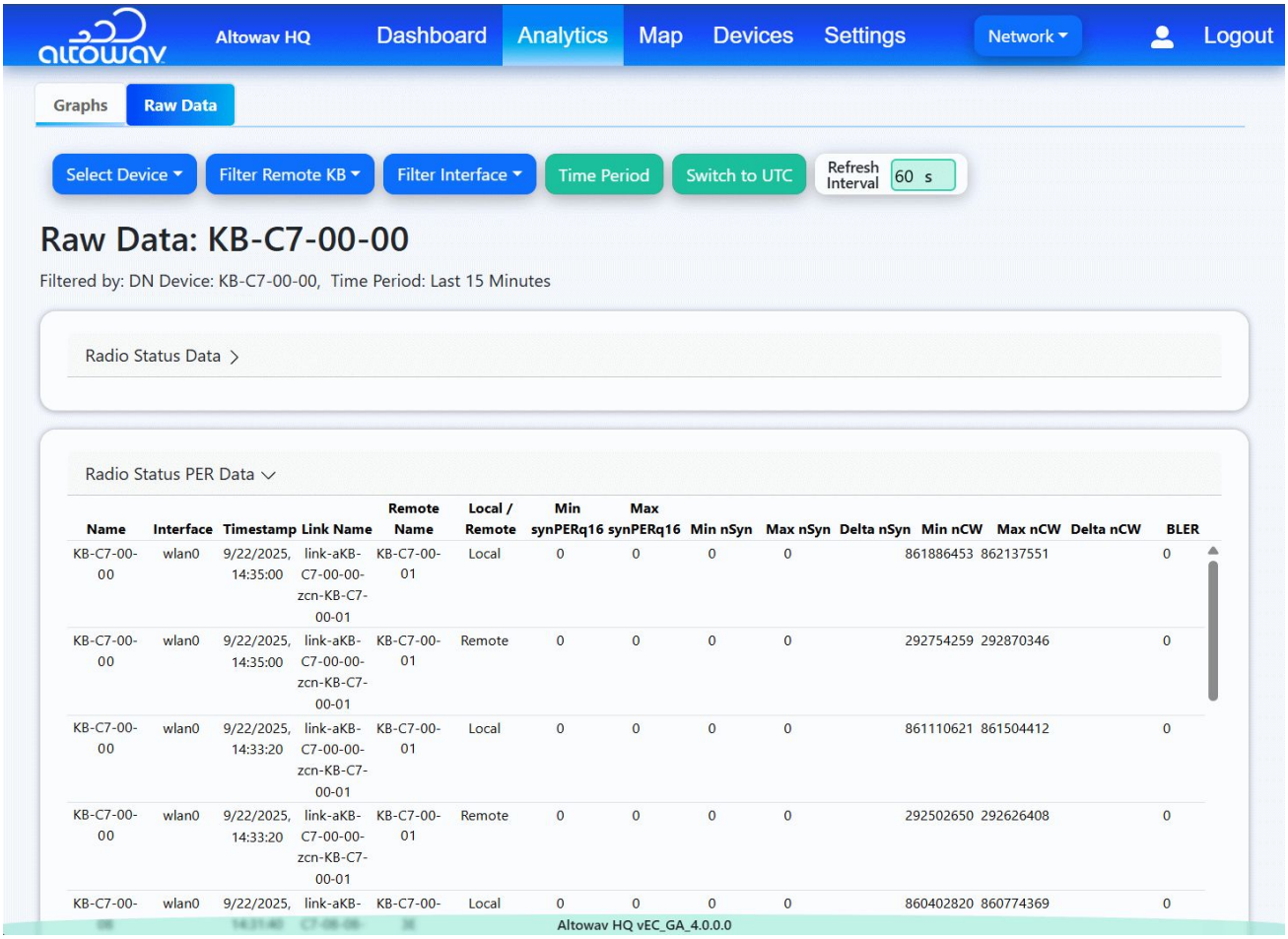
Refresh Interval (sec) - Set the interval for refreshing the graphs. 60 seconds is the minimum refresh interval. Setting the interval to 0 disables data refresh. Default is 0.

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.

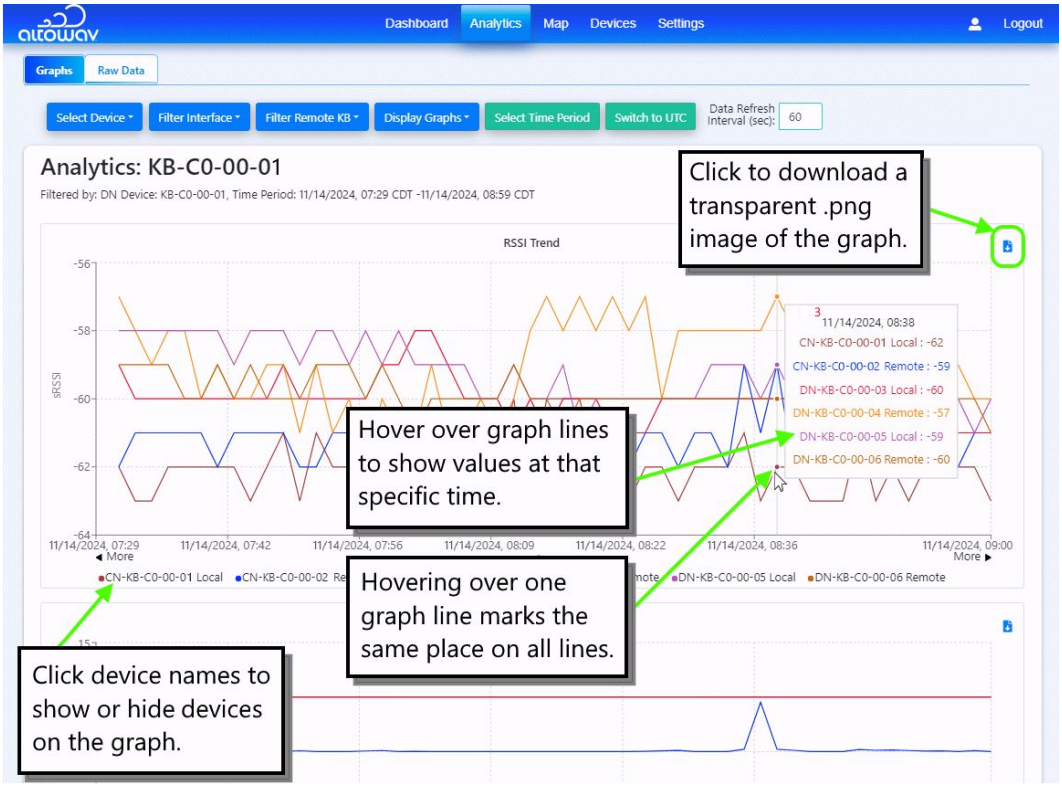
Click on the data categories to expand or collapse the data. For example, click on **Radio Status PER Data** to show the packet error rate data from Radio Status, filtered by the device, interface and time selected.



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 by clicking and release to select a time period. Click and drag along the x axis, then release to select the time period and to expand the graph to that time.

Enable intelligent rebeamforming

Rebeamforming is a process by which the beam that forms a wireless connection between two devices is reformed. 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 devices.

1. Open the AltoCommand WebUI:

   In your browser's address bar, type:

   https://*hostname*

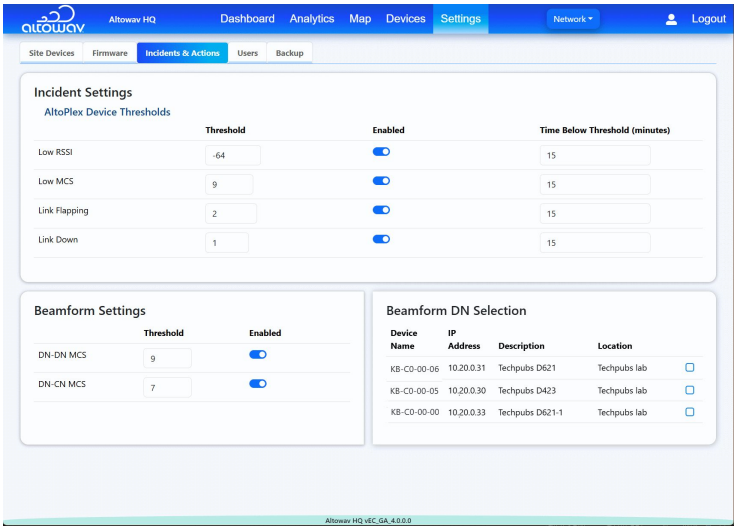
   where *hostname* is the fully qualified domain name of the AltoCommand server.

2. Log into the WebUI as a user with admin privileges.

   The default username is **admin**

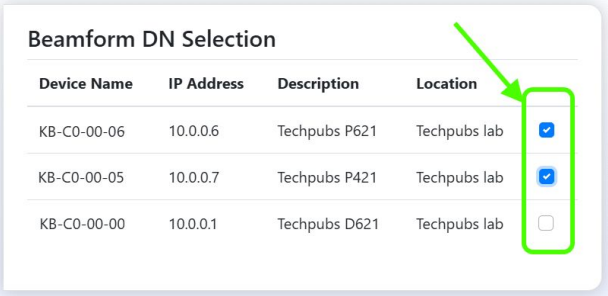
   The default password is **admin**

3. Click **Settings** > **Incidents & Actions**.



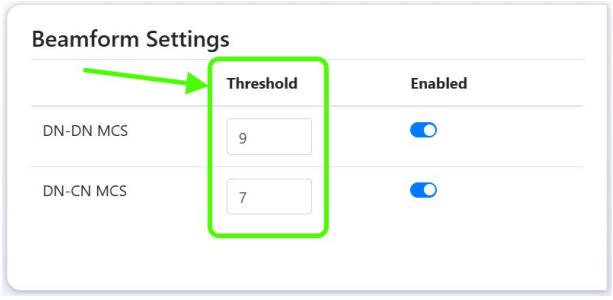
The **Incidents & Actions** page displays.

- 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, or both.

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.

Use AltoCommand to refine network performance

Even when overall network performance is good, best practice is 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

To review these performance metrics:

1. Open the AltoCommand WebUI:

   In your browser's address bar, type:

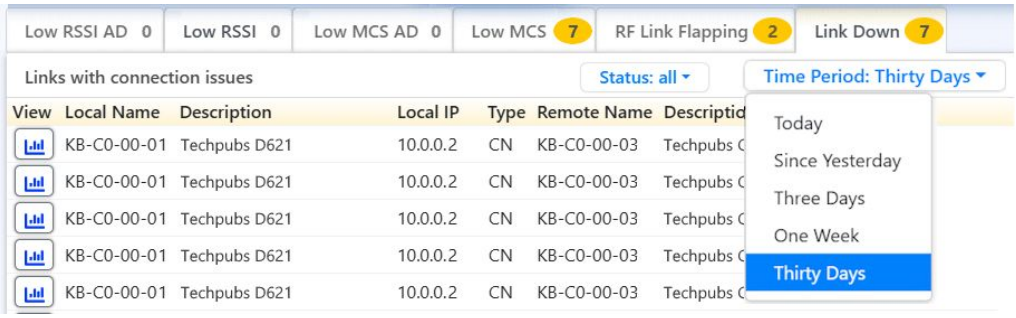
   https://*hostname*

   where *hostname* is the fully qualified domain name of the AltoCommand server.

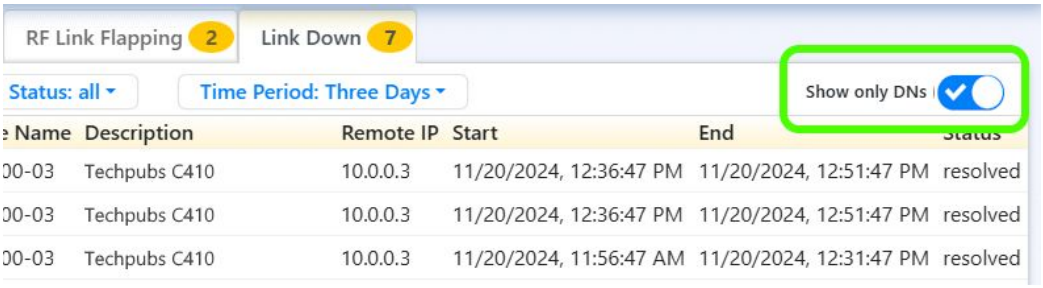
2. Log into the WebUI as a user with either user or admin privileges.

   The AltoCommand WebUI opens to the **Dashboard**.

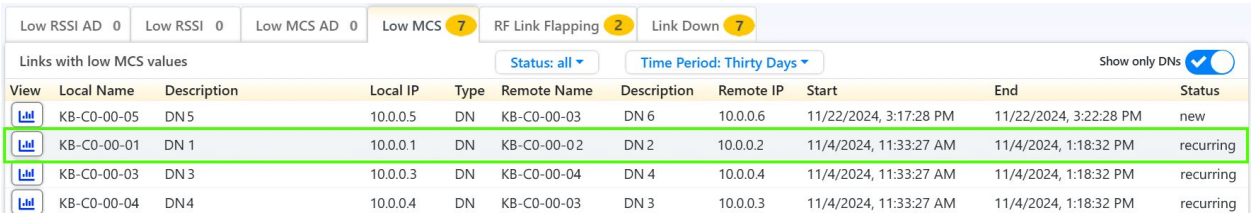
3. Select the **Incidents** tab.
4. Set the time period to **One Week** or **Thirty Days**.



5. Enable **Show only DNs**.



6. 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.



7. Click **Map** in the menu bar to use the Map to determine whether there are environmental factors that could be causing the issue. For example, check for:
    - Topology issues.
    - Fresnel zone interference.
    - Co-channel interference.
    - Radios that are off boresight.

Common Administrative Tasks

Fleet upgrade

Device upgrades can be performed on an individual basis, either from within AltoCommand or from the device WebUI (see Upgrade an individual device or see the device documentation). However, the recommended method for device upgrade is to perform a fleet upgrade.

With AltoCommand's fleet upgrade:

- You upload new device firmware to AltoCommand.
- Configure the target firmware version.
- Graphically view the current firmware version for all devices.
- Upgrade all devices that are not at the target firmware version.
- AltoCommand uses intelligent upgrade logic to minimize device downtime:
  - Upgrades devices in the correct sequence.
  - Ensures that devices are back online after upgrade before proceeding to subsequent devices.

Upload device firmware

To upload new device firmware to the AltoCommand server:

1. Open the AltoCommand WebUI:

   In your browser's address bar, type:

   https://*hostname*

   where *hostname* is the fully qualified domain name of the AltoCommand server.

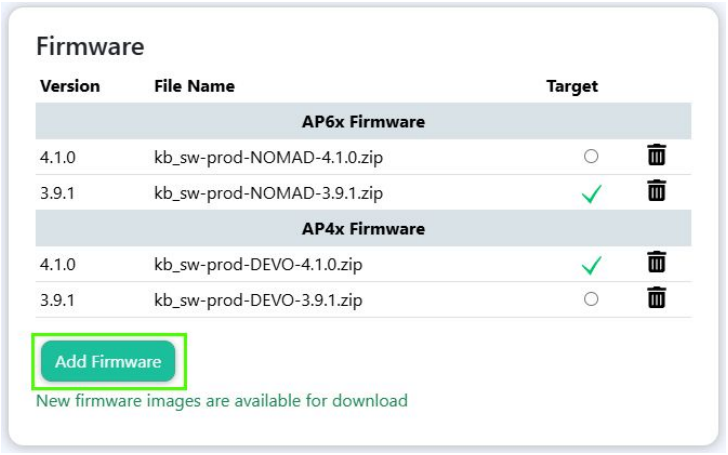
2. Log into the WebUI as a user with admin privileges.

   The default username is **admin**

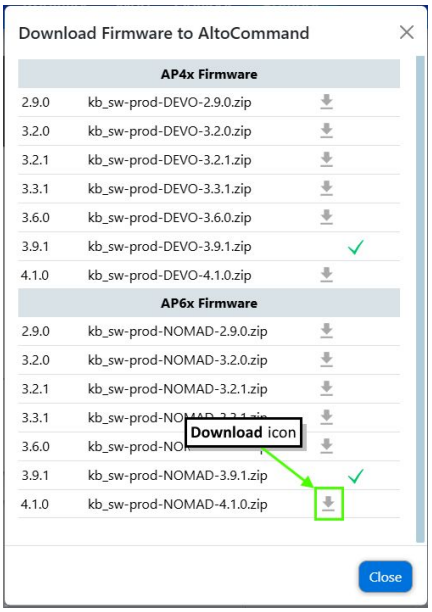
   The default password is **admin**

   The AltoCommand WebUI will open to the Dashboard's **Summary** page.

3. From the menu bar, click **Settings**.
4. Click the **Firmware** tab.
5. In the **Firmware** pane, click **Add Firmware**.



6. From the **Download firmware to AltoCommand** dialog, click the **Download** icon ( ) next to the appropriate firmware versions.
7. Click **Close** when complete.



The firmware binary filename

Note: Firmware is downloaded to AltoCommand in zip format. You do not need to unzip the files.

For AltoPlex devices, firmware is listed as **AP4x** or **AP6x**.

- **AP4x** — Firmware used for D423, C410, C420, and P421 devices.
- **AP6x** — Firmware used for D621 and P621 devices.

The firmware binary filename consists of three parts:

<*filetype*>-<*device_family_name*>-<*version_number*>.zip

where:

- *filetype* is **kb_sw-prod**
- *device_family_name* is one of:
  - **DEVO** — Firmware used for D423, C410, C420, and P421 devices.
  - **NOMAD** — Firmware used for D621 and P621 devices.
- *version_number* is the version number of the firmware.

For example:

kb_sw-prod-NOMAD-4.1.0.zip

Set the target firmware version

To set the target firmware:

1. Open the AltoCommand WebUI:

   In your browser's address bar, type:

   https://*hostname*

   where *hostname* is the fully qualified domain name of the AltoCommand server.

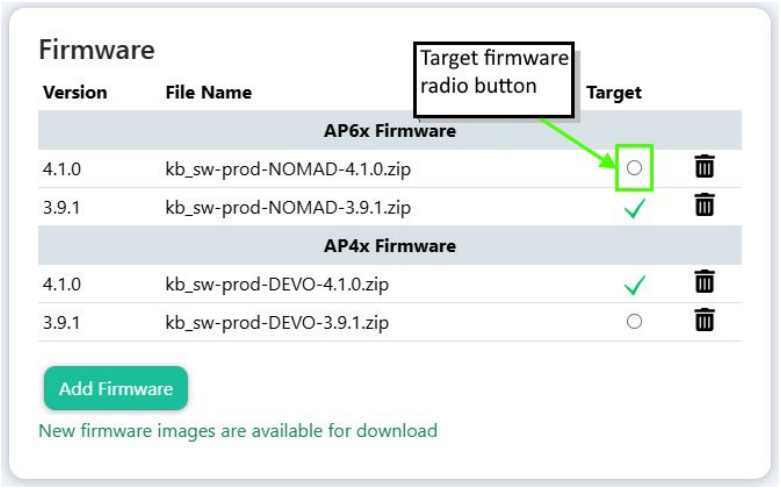
2. Log into the WebUI as a user with admin privileges.

   The default username is **admin**

   The default password is **admin**

   The AltoCommand WebUI will open to the Dashboard's **Summary** page.

3. From the menu bar, click **Settings**.
4. Click the **Firmware** tab.
5. In the **Firmware** pane, under Target, click the radio button for the appropriate target firmware. A checkmark will indicate that the firmware version is now the target version.



Delete existing firmware versions

You can also delete firmware from AltoCommand:

1. in the **Firmware** pane, click the **Delete** icon (🗑) next to the appropriate firmware file.
2. Click **Confirm** to confirm the deletion.

View firmware versions across your fleet of devices

You can view the current levels of firmware on devices in your Networks from the **Dashboard**:

1. Open the AltoCommand WebUI:

   In your browser's address bar, type:

   https://*hostname*

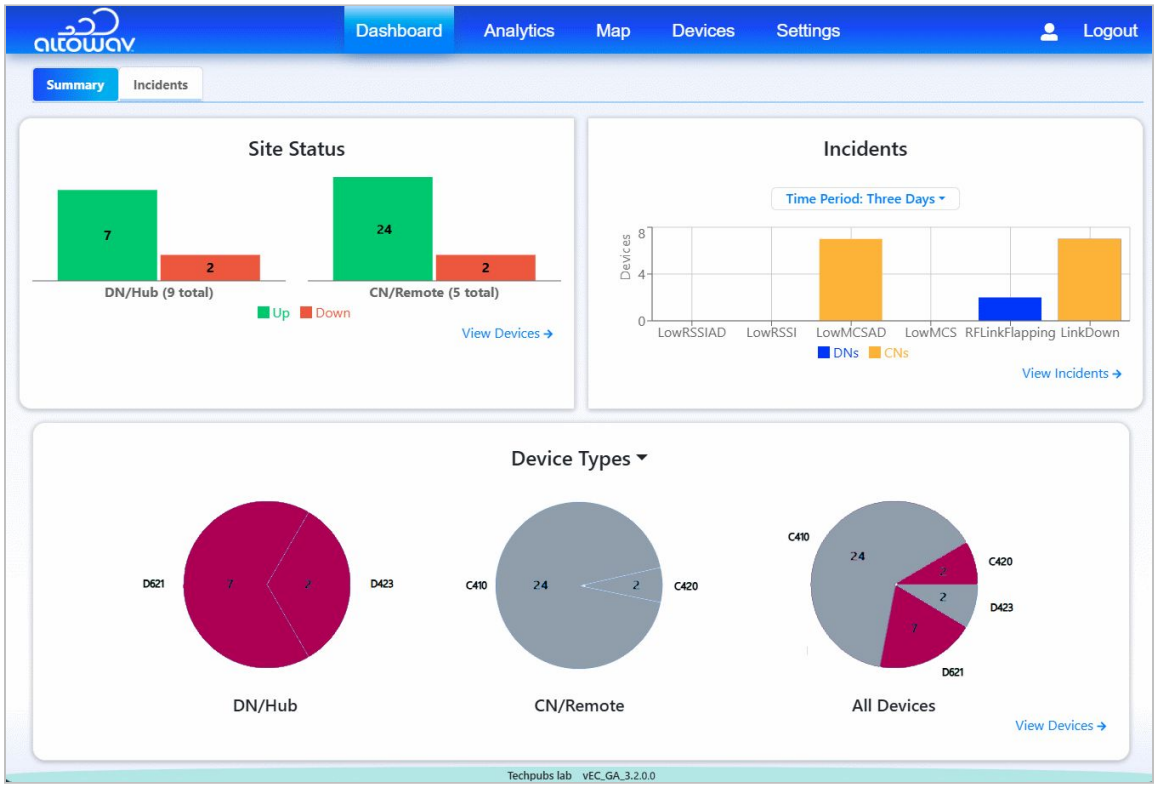
   where *hostname* is the fully qualified domain name of the AltoCommand server.

2. Log into the WebUI as a user with admin privileges.

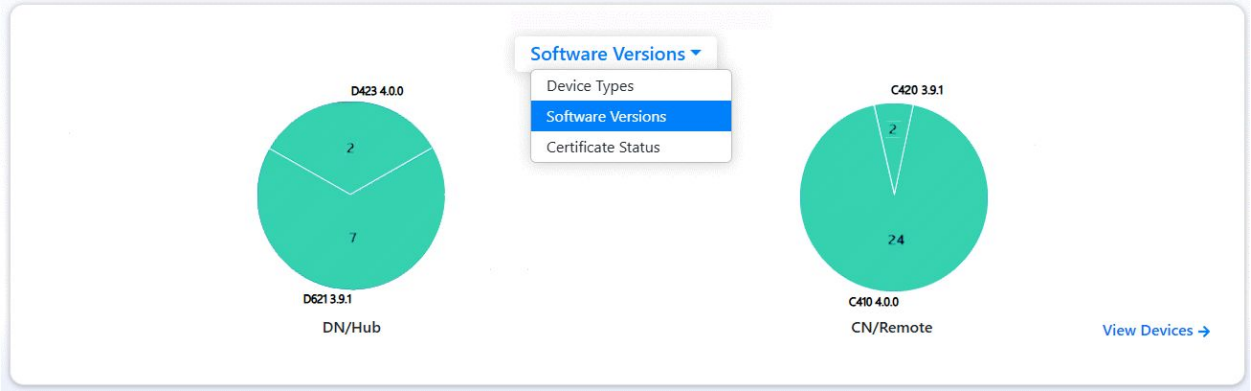
   The default username is **admin**

   The default password is **admin**

The AltoCommand WebUI will open to the Dashboard's **Summary** page.



3. In the dropdown for the **Device Types** pane, select **Software Version**.



Upgrade devices that are not at the target firmware version

The recommended way to upgrade devices is to use the fleet upgrade option, as described in this procedure. However, you can also upgrade devices individually, either from within AltoCommand or from the device WebUI (see Upgrade an individual device or see the device documentation).

1. Open the AltoCommand WebUI:

   In your browser's address bar, type:

   https://*hostname*

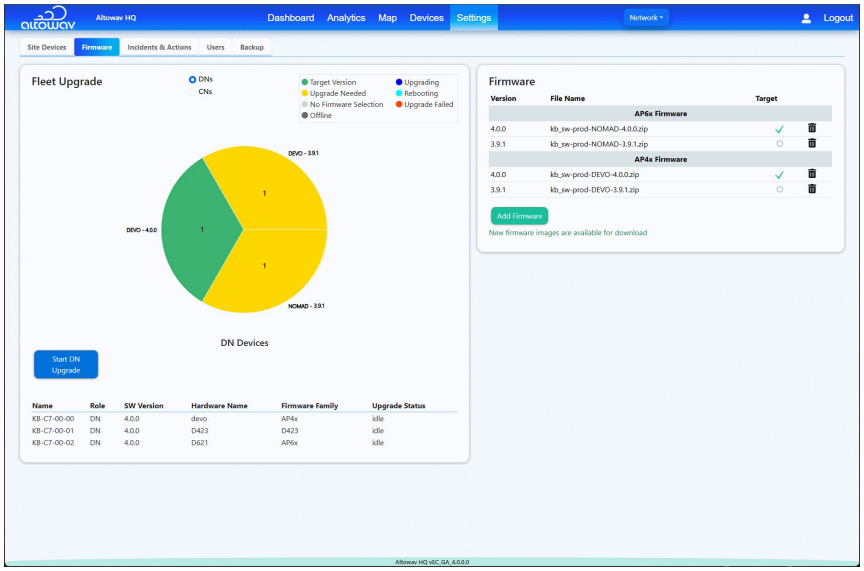
   where *hostname* is the fully qualified domain name of the AltoCommand server.

2. Log into the WebUI as a user with admin privileges.

   The default username is **admin**

   The default password is **admin**

   The AltoCommand WebUI will open to the Dashboard's **Summary** page.



3. From the menu bar, click **Settings**.
4. Click the **Firmware** tab.

5. To upgrade all DNs in your fleet that are not at the target level, click **Start DN Upgrade**.
6. To upgrade all CNs in your fleet that are not at the target level:
    A. Click the **CNs** radio button.
    B. Click **Start CN Upgrade**.

AltoCommand users

AltoCommand users can have one of two roles:

- 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 the current instance of AltoCommand.

Add users

To add a new user:

1. Open the AltoCommand WebUI:

   In your browser's address bar, type:

   https://*hostname*

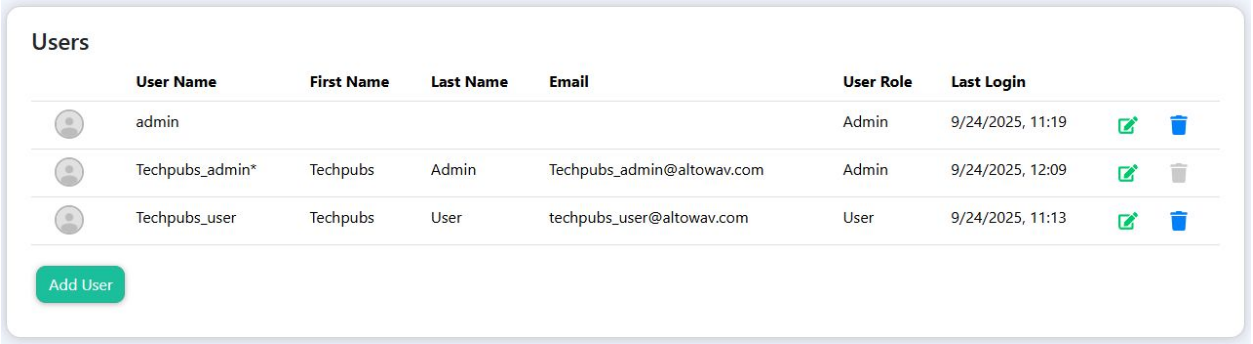
   where *hostname* is the fully qualified domain name of the AltoCommand server.

2. Log into the WebUI as a user with admin privileges.

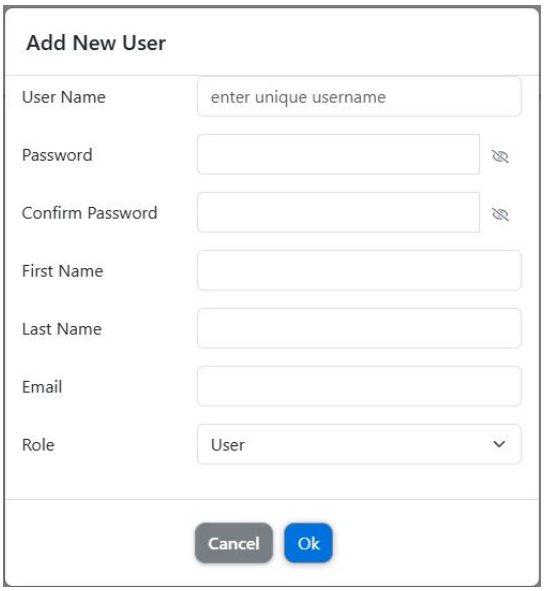
   The default username is **admin**

   The default password is **admin**

3. Click **Settings** > **Users**.



4. Click **Add User**.



   - **Username**:
     - Must be unique (no other users with the same username).
     - Minimum of four characters.
     - Maximum of 256 characters.
     - No whitespace characters.
   - **Password**:
     - A minimum of eight characters.
     - Cannot start or end with a whitespace.
   - **First Name** and **Last Name**: (Optional) The name of the user.
   - **Email**: (Optional) The user's email address.
   - **Role**:
     - **User**: Read-only access to AltoCommand, with the exception that they can edit their own user information and change their password.
     - **Admin**: Can perform write operations within the current instance of AltoCommand.
5. Click **OK**.

Delete an existing user

To delete an existing user, in the **Settings** > **Users** tab, click the **Delete** icon ( ).

Edit user information

Note: Usernames cannot be changed. To change a user's username, an admin user must delete the existing user configuration and create a new one using the new username.

Information that can be changed varies depending on the role of the user:

- Individual users can change the following settings for their user configuration:
  - First and last names (not username).
  - Email address.
  - Timezone settings.
- Users with admin privileges can edit user information for any user configured on the AltoCommand server. Admin users can change a user's:
  - First and last names (not username).
  - Email address.
  - User role.

See Change the password of an AltoCommand user for information about how to change a user's password.

Change the user information of the current user

To change the user information of the current user:

1. Open the AltoCommand WebUI:

   In your browser's address bar, type:

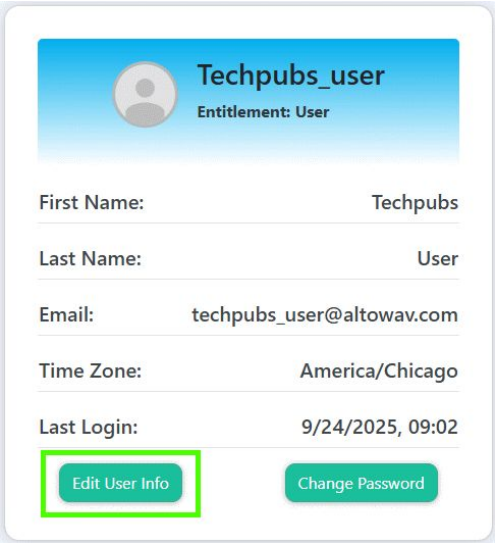
   https://*hostname*

   where *hostname* is the fully qualified domain name of the AltoCommand server.

2. Log into the WebUI as a user with either user or admin privileges.

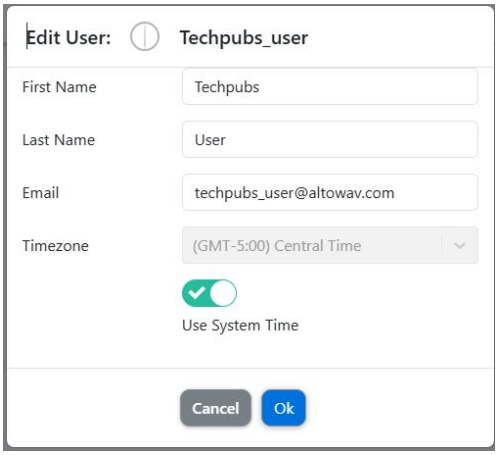
3. Click the **User** icon ( ).

   The **User** window opens.



4. Click **Edit User Info**.

   The **Edit User** dialog opens.



   A. Type a new **First Name**, **Last Name**, and **Email**.

   B. Changing the **Timezone** is useful when the user is monitoring a remote Network that is in a different timezone than the user. By setting the user's timezone to the same timezone as the Network, timestamps in AltoCommand will reflect the timezone of the Network, rather than the timezone of the user.

      To set the timezone:

      i. Click to toggle off **Use System Time**.

         This will instruct AltoCommand to disregard the timezone settings of the user's local PC, and use the timezone configured here instead.

      ii. Select the **Timezone**.

   C. Click **Ok**.

Change user information of any AltoCommand user

To change user information for any user on the system, you must be logged in as a user with admin privileges.

1. Open the AltoCommand WebUI:

   In your browser's address bar, type:

   https://*hostname*

   where *hostname* is the fully qualified domain name of the AltoCommand server.

2. Log into the WebUI as a user with admin privileges.

   The default username is **admin**

   The default password is **admin**

3. Click **Settings** > **Users**.

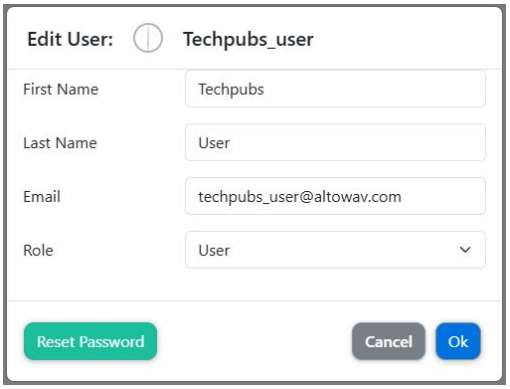
4. Click the **Edit** icon ( ).

   The **Edit User** dialog opens.

   A. Type a new **First Name**, **Last Name**, and **Email**.

   B. Select the user role.

   C. Click **Ok**.



Change the password of an AltoCommand user

Individual AltoCommand users can change their own password, and users with admin privileges can change the password of any user on the system.

Change the password of the current user

To change the password of the user currently logged into AltoCommand:

1. Open the AltoCommand WebUI:

   In your browser's address bar, type:

   https://*hostname*

   where *hostname* is the fully qualified domain name of the AltoCommand server.

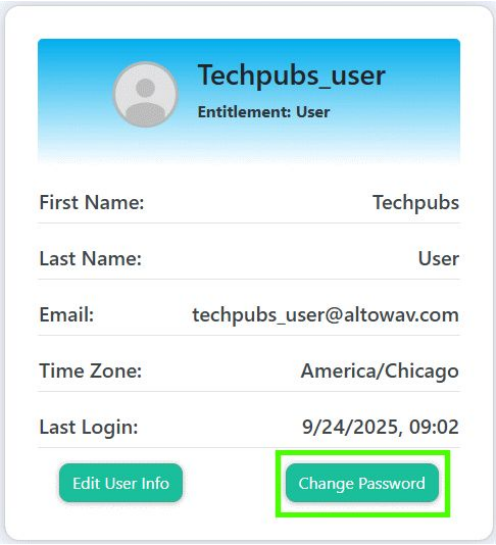
2. Log into the WebUI as a user with either user or admin privileges.

3. Click the **User** icon ( ).

   The **User** window opens.

4. Click **Change Password**.

5. Type and confirm the new password and click **OK**.



Change the password of any AltoCommand user

To change password for any user on the system, you must be logged in as a user with admin privileges.

1. Open the AltoCommand WebUI:

   In your browser's address bar, type:

   https://*hostname*

   where *hostname* is the fully qualified domain name of the AltoCommand server.

2. Log into the WebUI as a user with admin privileges.

   The default username is **admin**

   The default password is **admin**

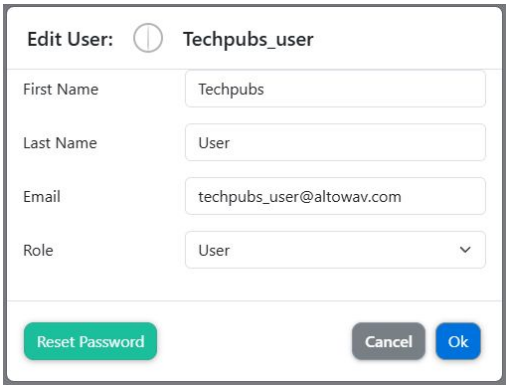
3. Click **Settings** > **Users**.

4. Click the **Edit** icon ( ).

   The **Edit User** dialog opens.

5. Click **Reset Password**.

6. Type and confirm the new password and click **OK**.



Change the user's timezone

Changing a user's timezone is useful when the user is monitoring a remote Network that is in a different timezone than the user. By setting the user's timezone to the same timezone as the Network, timestamps in AltoCommand will reflect the timezone of the Network, rather than the timezone of the user.

1. Open the AltoCommand WebUI:

   In your browser's address bar, type:

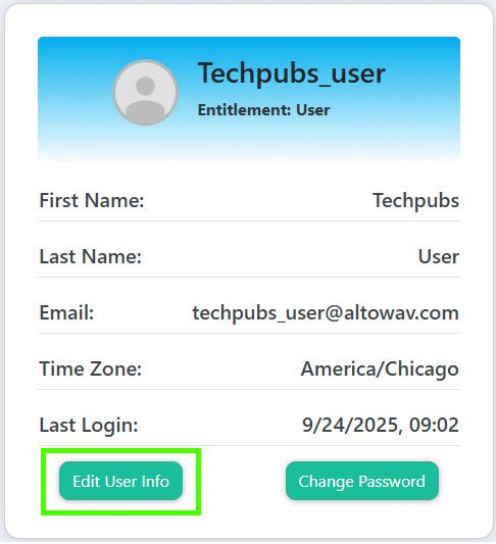
   https://*hostname*

   where *hostname* is the fully qualified domain name of the AltoCommand server.

2. Log into the WebUI as a user with either user or admin privileges.

3. Click the **User** icon ( ).

   The **User** window opens.



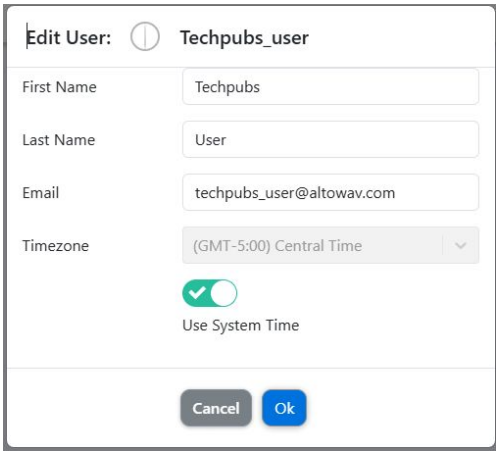
4. Click **Edit User Info**.

   The **Edit User** dialog opens.

5. Click to toggle off **Use System Time**.

   This will instruct AltoCommand to disregard the timezone settings of the user's local PC, and use the timezone configured here instead.

6. Select the **Timezone**.
7. Click **Ok**.



Back up and restore AltoCommand certificate files

AltoCommand uses certificate-based authentication to have write-enabled access to AltoPlex devices. If your AltoCommand server fails, you can restore a backup of the AltoCommand certificates to a new AltoCommand server.

To backup and restore the AltoCommand certificates:

1. Open the AltoCommand WebUI:

   In your browser's address bar, type:

   https://*hostname*

   where *hostname* is the fully qualified domain name of the AltoCommand server.

2. Log into the WebUI as a user with admin privileges.

   The default username is **admin**

   The default password is **admin**

3. Click **Settings** > **Backup**.
4. To download backup copies of the certificates used by AltoCommand, click **Download Backup**.

   A zip file containing the certificate backups will download.

5. To restore certificates, click **Choose file** and select the zip file that contains the backed up certificates. Click **Restore from Backup**.

Using K60 devices with AltoCommand

Depending on the release level of your AltoCommand server, the server supports supports certain variants of earlier Gen2 Altowav devices.

- Gen2 devices supported with AltoCommand release 4.x and newer:
  - K60 (both Hub and Remote roles). Must be at release 3.21 or later.
- AltoCommand release 3.x and older:
  - K60
  - K60c
  - K60c+
  - K60i
  - K60x

This guide covers AltoCommand release 4.x and newer. For information about AltoCommand release 3.x and older, see the AltoCommand Version 3.x User Guide.

Note: Altowav does not recommend blending K60 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 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
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
Initial Map Positioning	DNs with GPS available and enabled are auto positioned on the **Map**.	CNs with GPS available and enabled are auto positioned on the **Map**. CNs without GPS are added to the **Map**, near their connected DN.	No GPS available. **Hubs** require manual positioning on the Map. **Remotes** are added to the Map, near their connected Hub.

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.

Boresight — Proper parallel alignment. For radio technology, this refers to the antennas of two radios facing directly at each other.

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.

Co-channel interference — A situation where radio waves on the same channel interfere with each other, leading to degraded signal quality and performance loss.

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 .

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.

Fresnel zone — An elliptical area surrounding the line of sight between two radios. The Fresnel zone should be clear of all obstruction to guarantee the strongest signal. For a 400 meter 60 GHz link, the Fresnel zone at its widest point at 200m is 1.5m in diameter.

FWA — See Fixed wireless access.

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

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

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

Initiator — The that initially establishes a link with a remote device. By default, the 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 the beam that forms a wireless connection between two devices is reformed.

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.