Dart RTLS
User Guide

Document D2119 Rev F Dart RTLS User Guide

Liability Disclaimer

Zebra Enterprise Solutions takes steps to ensure that its published documentation is correct; however, errors do occur. Zebra Enterprise Solutions reserves the right to correct any such errors and disclaims liability resulting there from.

Limitation of Liability

In no event shall Zebra Enterprise Solutions or any of their licensors be liable to for any of the following (collectively referred to as "Injuries"): injuries (including death) or damages to persons or to property, or damages of any other kind, direct, indirect, special, exemplary, incidental or consequential, including, but not limited to, loss of use, lost profits, lost revenues, loss of data, replacement costs, debt service or rental payments, or damages owing by You to others, whether arising out of contract, tort, strict liability or otherwise, arising from or relating to the design, use or operation of these online materials, the Software, Documentation, Hardware, or from any Services provided by Zebra Enterprise Solutions (whether or not Zebra Enterprise Solutions or its licensors knew or should have known of the possibility of any such Injuries) even if a remedy set forth herein is found to have failed of its essential purpose.

Zebra Enterprise Solutions Corp.
2940 N 1st Street
San Jose CA 95134 USA
http://zes.zebra.com
Tel: +1 408 473 8500
Fax: +1 408 473 8501

Contents

1 General Description

The Dart Real Time Locating System (RTLS) Ultra-Wideband (UWB) system is designed for the tracking of personnel and/or equipment. A base system is defined as one Hub, four or more Receivers, one or more reference tags, and multiple DartTags for tracking individual assets or personnel.

In This Section

Concept of operation

Dart RTLS uses short pulse Ultra-Wideband (UWB) technology to determine the precise location of UWB radio frequency identification (RFID) tag.

Each DartTag repeatedly sends out a packet burst consisting of a short train of UWB pulses, Dart UWB Receivers receive these transmitted UWB pulses. Receivers are typically located about the periphery of the area of coverage. Reception by three or more Receivers permits accurate 2-D localization.   If only one Receiver receives a tag transmission, this can report proximity detection.

To determine the actual tag position from these measurements, the Dart Hub, using calibration data from a reference tag, determines the differential times of arrival between Receivers.

The Dart Hub performs several other functions as well:

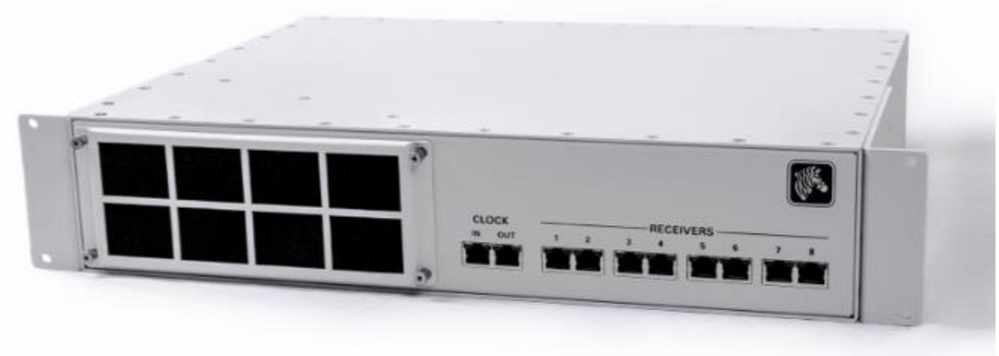
- It serves as a source of DC power to the individual Receivers
- It provides a stable clock reference to each Receiver, allowing individual Receivers to be frequency-locked for high measurement stability (US Patent 6,882,315).
- It incorporates a graphical user interface (GUI) and communication ports for client access to the location data.

Dart RTLS Hub

The Dart RTLS Hub houses a single board CPU that:

- Interprets the data sent from the Receivers.
- Generates the identity and location of each DartTag within a designated area.
- The Hub LAN interface makes the results available to client computers for further processing and display.

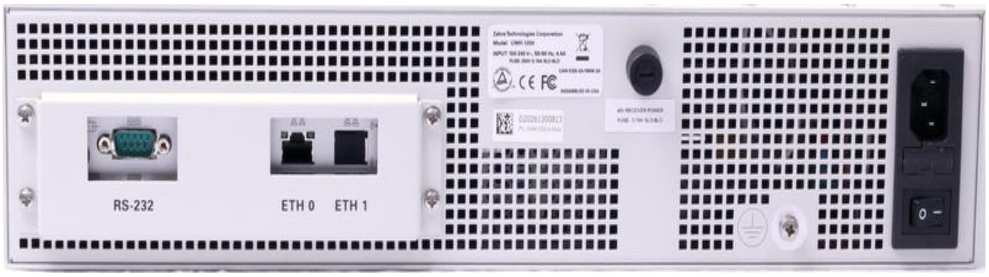
The following figure shows the front view of the Dart RTLS Hub.



The Hub accepts input power of 100-240 Volts AC and provides power to the Receivers over a CAT 5E cable. The same CAT 5E cable sends a clock source and serial communication data to the Receivers. The front panel of the Hub has eight RJ45 connectors that are used for connecting Receivers to the Hub. The Hub is capable of localizing Dart Tags with up to 64 Receivers per Hub. Zebra recommends that you distribute the receivers among the ports to balance the communication load.

⚠ Use care to only connect Receivers to the Hub port connectors on the front panel and to only connect LAN cables to the Ethernet port connector on the rear panel. Improper connections may result in damage to Receivers, Hub or external LAN equipment.

The following figure shows a rear view of the Dart RTLS Hub.



The Hub chassis is enclosed in a metal case with optional rack mount brackets. The rear panel of the Hub has an Ethernet interface ETH0 (accessible through an IP network) for configuring the Hub and passing output information over the LAN. ETH1 is disabled and should not be used.

Dart RTLS Receiver

Dart RTLS Receivers operate with a nominal center frequency of 6.55 GHz. The Receiver detects pulses from the DartTags and generates packets of information, which are in turn sent to the Hub over a CAT5E cable.

You can connect the Receivers directly to a Hub port connection or in a daisy chain to other Receivers. Each Receiver receives 48VDC from the previous Receiver (or from the Hub if it is the first Receiver in the line) and passes the 48VDC on to the next Receiver in line via the CAT 5E cable.

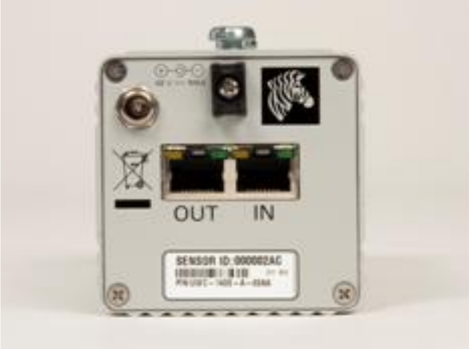
Similarly, each Receiver receives a clock and bi-directional data from the previous Receiver (or from the Hub if it is the first Receiver in the line) and passes these on to the next Receiver in line.

The following figure shows Dart RTLS Receivers.

The back of each Receiver includes two RJ45 connectors, as shown in the following figure, one to connect to the previous Receiver or Hub in the line (labeled IN) and one to connect to the next receiver in line (labeled OUT). When the Receiver is getting power, a yellow LED flashes on when data is being read from the Receiver.

The flashing may be too short to be noticed when data traffic is high.

Each Receiver requires approximately 35ma at 48VDC, which is supplied by the previous Receiver in the line (labeled IN) or the Hub.



Each Receiver has:

- An auxiliary DC connection that supplies additional power to the Receiver when Hub power is not adequate (not typically used).

Use of Zebra external power supply is limited to indoor use and a max 40°C environment. External power supplies should power a maximum of 6 Receivers per power supply. Only use Zebra approved power supplies.

- A unique 4-byte hexadecimal ID that is programmed by the factory into the Receiver. This unique Receiver ID is used to identify the Receiver in the Dart Hub configuration.

DartTags

The DartTags are UWB transmit-only devices that communicate wirelessly with the Receivers.

They have a nominal center frequency of 6.55 GHz with a peak and average power compliant with FCC Part 15 regulations. The DartTags are powered with a 3V battery with a life expectancy proportional to the size of the battery. The following form factors are currently available for tags:

- DartTags for mounting on assets
- DartTags for personnel tracking

Reference tag

Every Dart RTLS Hub requires at least one reference tag for computing positions and synchronizing the counting functions inside the Receivers. Zebra recommends the DartTag asset tag form factor for the reference tag.

You must place each reference tag in a stationary position such that at least two Receivers connected to a given Hub have an unobstructed path to it. To minimize the number of reference tags required in your system, carefully position each tag to maximize its visibility. The reference tag should be visible to as many Receivers as possible. The position of each reference tag must be accurately known.

2 Unpacking Dart RTLS

Typically, a Dart RTLS System is shipped with the following items:

- Dart RTLS Hub, with mounting brackets and power cord
- Dart Receivers
- DartTags

To unpack Dart RTLS:

1. Open the shipping container and carefully remove the contents.
2. Return all packing materials to the shipping container and save it.
3. Ensure that all items listed above are included in the shipment.
4. Check each item for damage.

⚠ Prior to installing the AC cable make sure the power switch on the back of the hub is "Off" (in the 0 position). Push the rocker 0/1 switch to the 0 position to ensure that.

⚠ Prior to turning the power "Off" make sure to shut down the hub processor as described in the Hub administration section (section 8)

3 Installing the Dart RTLS hardware

⚠ Before installation, review the **Safety and Installation Warnings and Cautions** document – D26819.

Dart RTLS is a precision tracking system and requires a degree of exactness in installation. Specifically, the Receiver and reference tag locations are critical to insure optimum performance. The accuracy of these positions directly influences the accuracy of the results.

When installing Dart RTLS, you may need the following equipment:

- Measurement device (for laying out an accurate X-Y grid)
- Optional, Receiver-mounting brackets and associated hardware for affixing Receivers to the wall or ceiling
- Computer to access the Hub software
- 10/100/1000 Base-T Ethernet Hub for Ethernet Network connectivity

⚠ For safety-related installation requirements, see the document *Safety and Installation Warnings and Cautions*.

In This Section

Placing the Dart RTLS Hub

You must place the Dart RTLS Hub:

- Within 1000 feet of the first Receiver in the Receiver chain.
- In a location where either LAN or computer connection is available.

Placing the Receivers

Identify the physical area to be covered. You can configure the system with a single Receiver if tag detection (presence) only is required. To identify the x-y positions of one or more assets, you need a minimum of three Receivers.

The ideal installation is a rectangular box with Receivers in each of the four corners, installed as high as possible (near the ceiling) and with the antenna of each Receiver pointing towards the center of the box.

Placing the cables

You can install a cable in the open or install it professionally. Zebra recommends that you check all cable connections with a cable tester prior to installing the system. Cable end breakage during installation is a common troubleshooting problem. Cables could be shielded or un-shielded CAT 5E cables (shielded/un-shielded CAT 6 cables are also acceptable), 24AWG (or heavier gauge) is recommended for best results. Stranded or solid cables are acceptable. The cable length limits the distance between the Receivers. The maximum distance hub-to-Receiver or Receiver-to-Receiver is 1000 feet.

For more information, see:

- ***Appendix: Shielded CAT 5E cable recommendations*** (on page 126)
- ***Appendix: Dart RTLS cabling guidelines*** (on page 133)

Positioning the reference tag

In the area to be monitored, you must position the reference tag in a position that each of the Receivers can see easily. The optimal location for the reference tag is in the center of the box formed by the Receivers. Each Receiver must have a direct line of sight to the reference tag. The reference tag must be in a position where it cannot easily be moved or obstructed during operation.

Hardware Compatibility

All Dart Receivers (UWC-1100, UWC-1200, UWC-1300, UWC-1400 and UWB-1450) are compatible with the UWH-1200. For best results, Zebra recommends part numbers ending with -00AB or above.

All Zebra UWB tags are compatible with the UWH-1200.

4 Connecting the Receiver cables

You can connect Receivers directly to a Hub port connection or in a daisy chain to other Receivers. Each Receiver receives 48VDC from the previous Receiver (or from the Hub, if it is the first Receiver in the line) and passes the 48VDC on to the next Receiver in line via the CAT 5E cable. Location data throughput varies depending on the configuration of the receivers.

The following sections guide you through connecting the Receivers:

- ***Directly to the Hub*** (on page 15) (star configuration)
- ***In a daisy chain to the Hub*** (on page 15)
- ***In series and parallel to the Hub*** (on page 16) (combined daisy chain and star configuration)

In This Section

Connecting Receivers directly to the Hub (star configuration)

You can connect the CAT 5E cables between the Dart RTLS Hub and the Receivers in a star configuration.

The Dart RTLS Hub supports the direct connection of eight individual Receivers.

To connect Receivers directly to the Hub:

1. Plug the RJ45 Ethernet connector of the first CAT 5E cable into one of the eight Hub connector ports marked RECEIVER on the front of the Dart RTLS Hub.
2. Repeat Step 1 for all remaining Receivers to connect to the Hub.

Connecting Receivers to the Hub (daisy chain configuration)

You can connect the CAT 5E power and data cables between the Dart RTLS Hub and the Receivers in a daisy chain.

To connect Receivers to the Hub in a daisy chain configuration:

1. Plug the RJ45 Ethernet connector of the first CAT 5E cable into one of the eight Hub connector ports marked RECEIVER on the front of the Dart RTLS Hub.
2. Connect the other end of the CAT 5E cable to the RJ45 connector marked "IN" of Receiver #1.
3. Connect a second CAT 5E cable to the RJ45 connector marked "OUT" of Receiver #1.

4 Connect the remaining end of the second CAT 5E cable to the RJ45 connector marked "IN" of Receiver #2.

5 Connect a third CAT 5E cable to the RJ45 connector marked "OUT" of Receiver #2.

6 Connect the remaining end of the third CAT 5E cable to the RJ45 connector marked "IN" of Receiver #3.

7 Connect the last (fourth) CAT 5E cable to the RJ45 connector marked "OUT" of Receiver #3.

8 Connect the remaining end of the fourth CAT 5E cable to the RJ45 connector marked "IN" of Receiver #4.

9 Continue to connect additional Receivers as required to the chain in series.

10 For optimal performance, evenly distribute receivers across all 8 hub ports.

Connecting Receivers in a star and daisy chain to the Hub

The Dart RTLS Hub supports a combination of daisy chain and star Receiver connections. To accomplish this, follow the appropriate steps:

- ***Star configuration*** (on page 15)
- ***Daisy chain configuration*** (on page 15)

5 Connecting multiple hubs

The Hubs can be connected in Daisy chain configuration to synchronize their clocks which will enable hubs to use receiver from other hubs whose clocks are in sync with each other. The front panel of the Hub has 2 RJ45 connectors that are used for clock synchronization marked as CLOCK IN and OUT. There are 8 other RJ45 connectors that are used for connecting receivers, (marked numbers 1 through 8 under RECEIVERS) to the hub.

The following sections guide you through connecting the Hubs:

⏩ ***In a daisy chain to the Hub*** (on page 15)

In This Section

⚠ Use care to only connect Receivers to the Hub port connectors on the front panel and to only connect LAN cables to the Ethernet port connector on the rear panel and use CLOCK IN and OUT for hub clock synchronizing. Improper connections may result in damage to Receivers, Hub or external LAN equipment.

⚠ For best result the Hubs used for clock synchronization and receiver sharing should be located on the same LAN subnet.

Connecting multiple Hub together in clock sync mode

You can connect the CAT 5E power and data cables between the Dart RTLS Hubs in a daisy chain.

To connect Hubs in a daisy chain configuration:

1. Plug the RJ45 Ethernet connector of the first CAT 5E cable into Hub#1 clock out port marked CLOCK OUT on the front of the Dart RTLS Hub.
2. Connect the other end of the CAT 5E cable to the RJ45 connector marked “CLOCK IN” of Hub #2.
3. Connect a second CAT 5E cable to the RJ45 connector marked “CLOCK OUT” of Hub#2.
4. Connect the remaining end of the second CAT 5E cable to the RJ45 connector marked “CLOCK IN” of Hub $3.
5. Continue to connect additional Hubs as required to the chain in series.

6 For optimal performance, the CAT 5E cable needs to be less than 1000 feet.

7 Limit number of hubs used for clock sync to 8.

⚠ DO NOT create a loop by connecting the last hub on the daisy chain back to first hub in the daisy chain. The result can be unpredictable and system will not function properly.

6 Connecting to the Dart RTLS Hub

Configuring and retrieving data requires a computer connection to the Dart RTLS Hub. You can connect the computer to the Hub through a direct connection or through a LAN. These are the default IP settings for the Hub:

IP Address	192.168.1.204
Subnet mask:	255.255.255.0
Default gateway address:	192.168.1.1

In This Section

System Requirements

The UWH-1200 firmware requires a JAVA™ Plug-in. If JAVA is not installed, you will be prompted to install the Java2 Runtime Environment (JRE version 1.6.0_23 or later) from the Oracle Technology Network website (http://www.oracle.com/technetwork/java/javase/downloads/index.html).

For Windows 7/8/8.1 computer, please refer the table below to select the right JRE to install.

Windows 7	Browser	JRE
64 Bits	32 Bits	32 Bits
64 Bits	64 Bits	64 Bits
32 Bits	32 Bits	32 Bits

For applications using maps using WMF (windows metafile format) or EMF (enhanced metafile format), you must also download Java Advanced Imaging, version 1.1.3, from http://download.java.net/media/jai/builds/release/1_1_3/jai-1_1_3-lib-windows-i586-jre.exe.

Connecting the Dart RTLS Hub to a PC through a LAN

If you can access the 192.168.1 subnet through your LAN, you can directly connect the Hub to the LAN.

To connect the Hub directly to your LAN:

1 Plug the RJ45 Ethernet cable into the Ethernet port on the back of the Dart RTLS Hub.

2 Connect the other end of the Ethernet cable to the LAN.

3 Plug the power cable in and turn the power on.

Connecting to a Dart RTLS Hub with an unknown IP address

If you do not know the IP address of the Hub, you may be able to connect through a terminal simulator application to obtain the IP address.

The UWH-1200 RS-232 port is a host male connector, to connect to a computer, a female to female null cable is required (such as L-com CSNULL9FF-5A WWW.L-COM.COM).

To connect the Dart RTLS Hub through the RS-232 serial port:

1 Connect the serial RS-232 port at the back of the Hub to your computer's serial port.

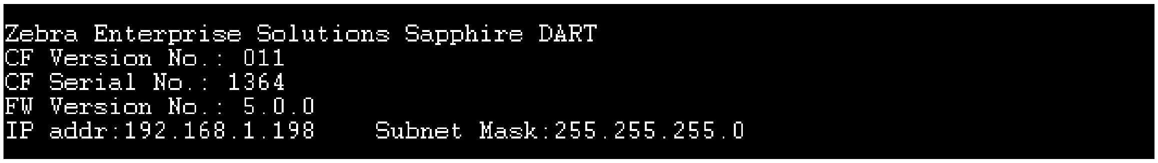
2 Run a terminal simulator application, such as HyperTerminal.

3 Set the serial port as follows:

Baud Rate: 115200
Data: 8 bit
Parity: None
Step: 1 bit
Flow Control: None

4 Connect to the Hub.

The terminal screen displays the IP address. In the example below, the IP address is 192.168.1.198.



```
Zebra Enterprise Solutions Sapphire DART
CF Version No.: 011
CF Serial No.: 1364
FW Version No.: 5.0.0
IP addr:192.168.1.198    Subnet Mask:255.255.255.0
```

Hub Administration and Management

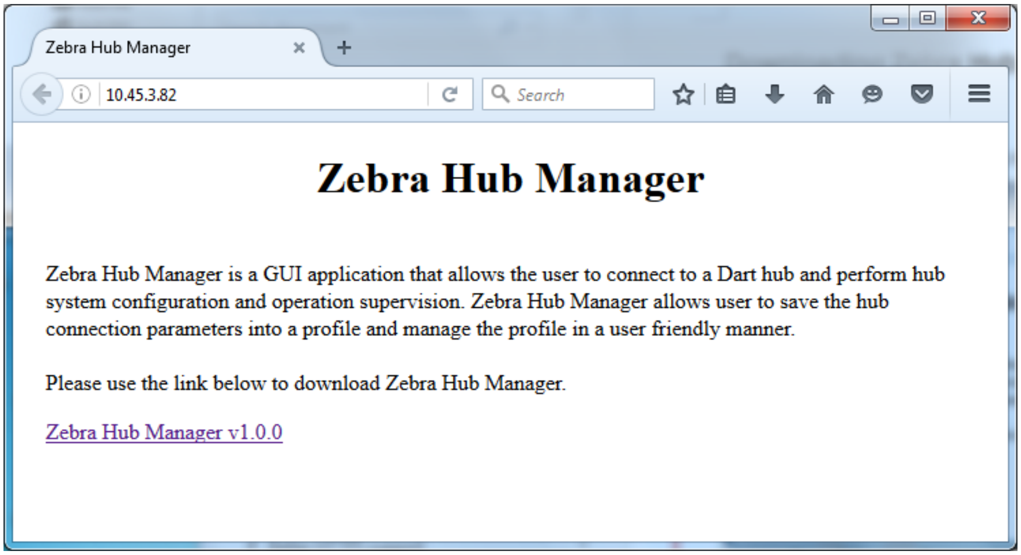
Accessing the Hub Administration and Management Application for the first time

Entering the IP address of the hub on a web browser used to take the user to the hub GUI web page where Hub Administration and Management tasks could be performed. For Hubs with FW Version 5.0.0 or higher, entering the IP address on a web browser will instead direct the user to a web page about Zebra Hub Manager, its usage and download link. With Zebra Hub Manager, the user will now be able to access the Hub Administration and Management application without needing a web browser. So the Hub GUI is essentially decoupled from the ever changing browser Java compatibilities. **The user still needs to have Java installed on the computer**.

Downloading Zebra Hub Manager using different browsers:

Mozilla Firefox:

- Enter the IP address of the hub and click on the link to Zebra Hub Manager



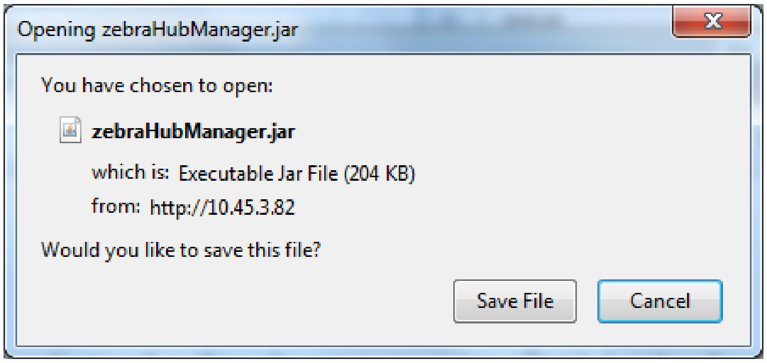
Zebra Hub Manager

Zebra Hub Manager is a GUI application that allows the user to connect to a Dart hub and perform hub system configuration and operation supervision. Zebra Hub Manager allows user to save the hub connection parameters into a profile and manage the profile in a user friendly manner.

Please use the link below to download Zebra Hub Manager.

Zebra Hub Manager v1.0.0

- Click **Save File** when Prompted


Opening zebraHubManager.jar

You have chosen to open:

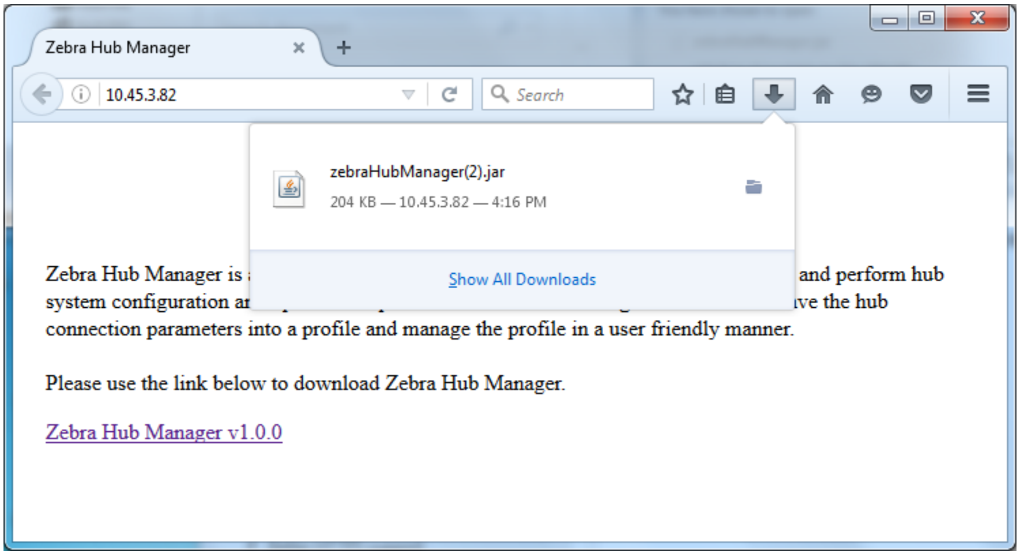
zebraHubManager.jar

which is: Executable Jar File (204 KB)

from: http://10.45.3.82

Would you like to save this file?

- Double click **ZebraHubManager.jar** in the download list of Firefox browser, or the Download folder to launch Zebra Hub Manager.



zebraHubManager(2).jar

204 KB — 10.45.3.82 — 4:16 PM

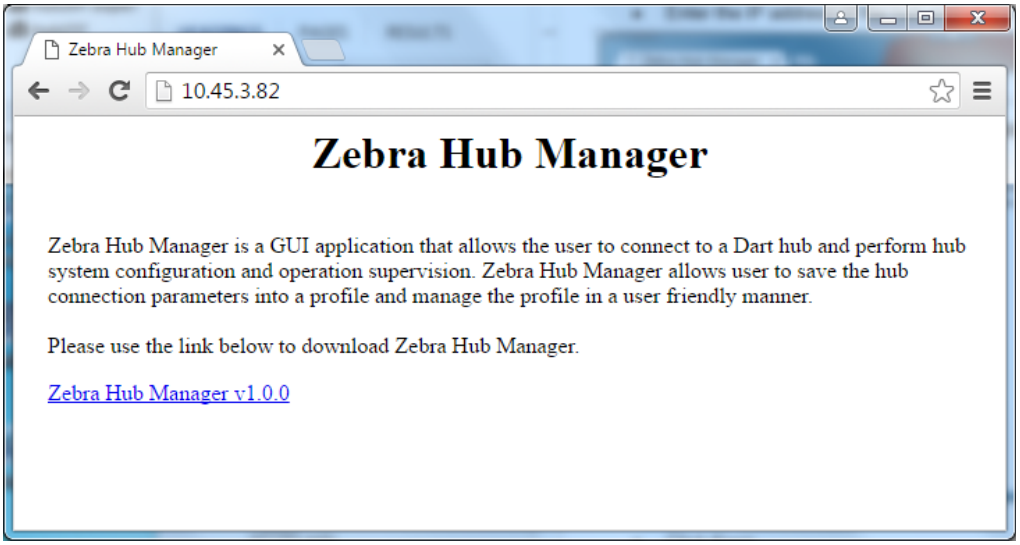
Zebra Hub Manager is a ... and perform hub system configuration a... ve the hub connection parameters into a profile and manage the profile in a user friendly manner.

Please use the link below to download Zebra Hub Manager.

Zebra Hub Manager v1.0.0

Google Chrome:

- Enter the IP address of the hub and click on the link to Zebra Hub Manager



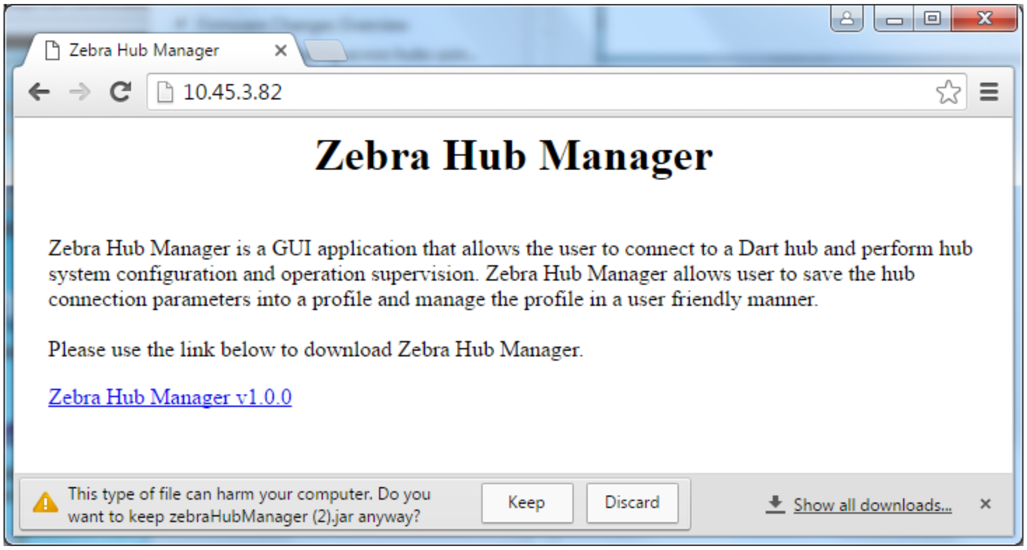
Zebra Hub Manager

Zebra Hub Manager is a GUI application that allows the user to connect to a Dart hub and perform hub system configuration and operation supervision. Zebra Hub Manager allows user to save the hub connection parameters into a profile and manage the profile in a user friendly manner.

Please use the link below to download Zebra Hub Manager.

Zebra Hub Manager v1.0.0

- Click **Keep**



Zebra Hub Manager

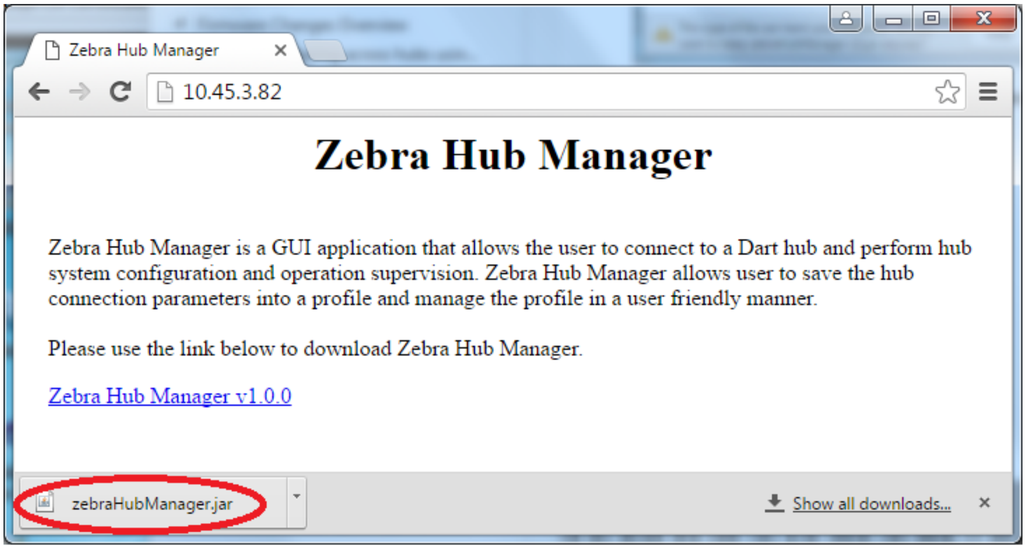
Zebra Hub Manager is a GUI application that allows the user to connect to a Dart hub and perform hub system configuration and operation supervision. Zebra Hub Manager allows user to save the hub connection parameters into a profile and manage the profile in a user friendly manner.

Please use the link below to download Zebra Hub Manager.

Zebra Hub Manager v1.0.0

This type of file can harm your computer. Do you want to keep zebraHubManager (2).jar anyway?

- Double click on **zebraHubManager.jar** to launch or look up zebraHubManager.jar in Download folder and double click on it to launch.



Zebra Hub Manager

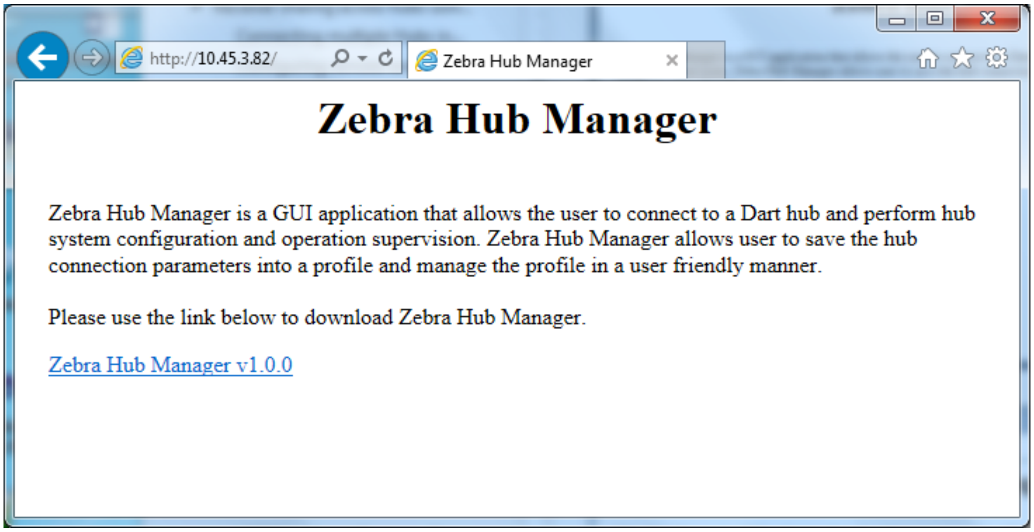
Zebra Hub Manager is a GUI application that allows the user to connect to a Dart hub and perform hub system configuration and operation supervision. Zebra Hub Manager allows user to save the hub connection parameters into a profile and manage the profile in a user friendly manner.

Please use the link below to download Zebra Hub Manager.

Zebra Hub Manager v1.0.0

Internet Explorer:

- Enter the IP address of the hub and click on the link to Zebra Hub Manager



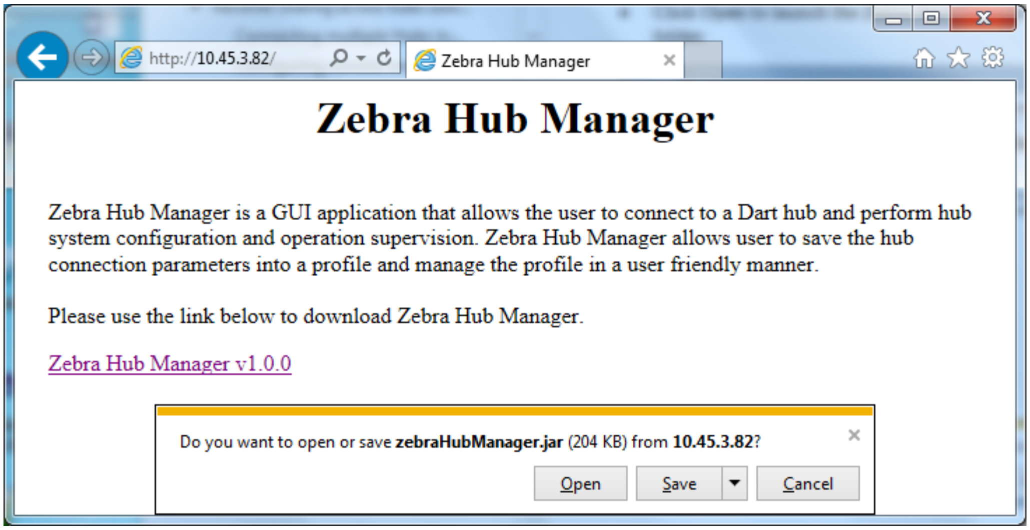
Zebra Hub Manager

Zebra Hub Manager is a GUI application that allows the user to connect to a Dart hub and perform hub system configuration and operation supervision. Zebra Hub Manager allows user to save the hub connection parameters into a profile and manage the profile in a user friendly manner.

Please use the link below to download Zebra Hub Manager.

Zebra Hub Manager v1.0.0

- Click **Open** to launch the Zebra Hub Manager or **Save** to save zebraHubManager.jar to Download folder.



Zebra Hub Manager

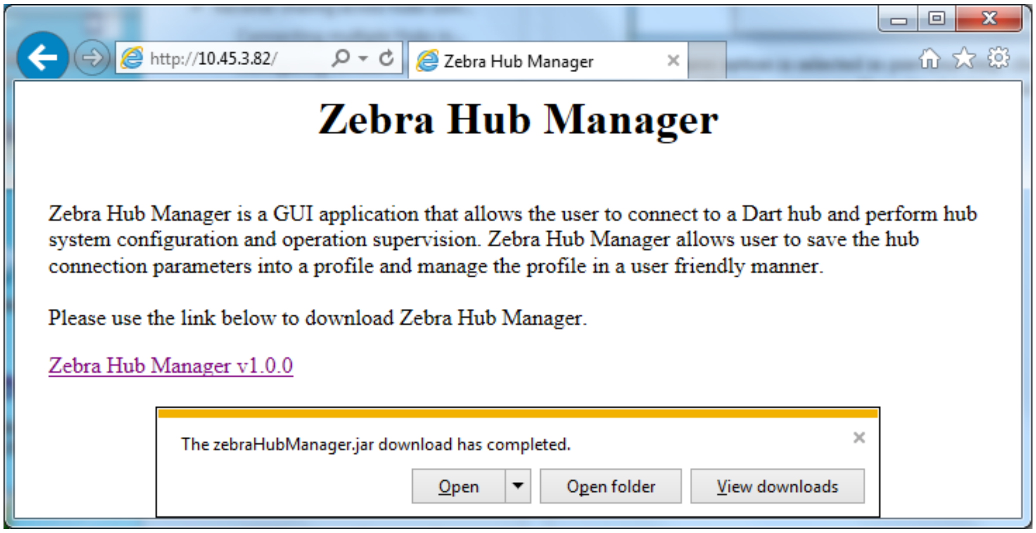
Zebra Hub Manager is a GUI application that allows the user to connect to a Dart hub and perform hub system configuration and operation supervision. Zebra Hub Manager allows user to save the hub connection parameters into a profile and manage the profile in a user friendly manner.

Please use the link below to download Zebra Hub Manager.

Zebra Hub Manager v1.0.0

Do you want to open or save **zebraHubManager.jar** (204 KB) from **10.45.3.82**?

- If **Save** option is selected in previous step, click **Open** to launch Zebra Hub Manager or look for zebraHubManager.ja in Download folder and double click to launch.



Zebra Hub Manager

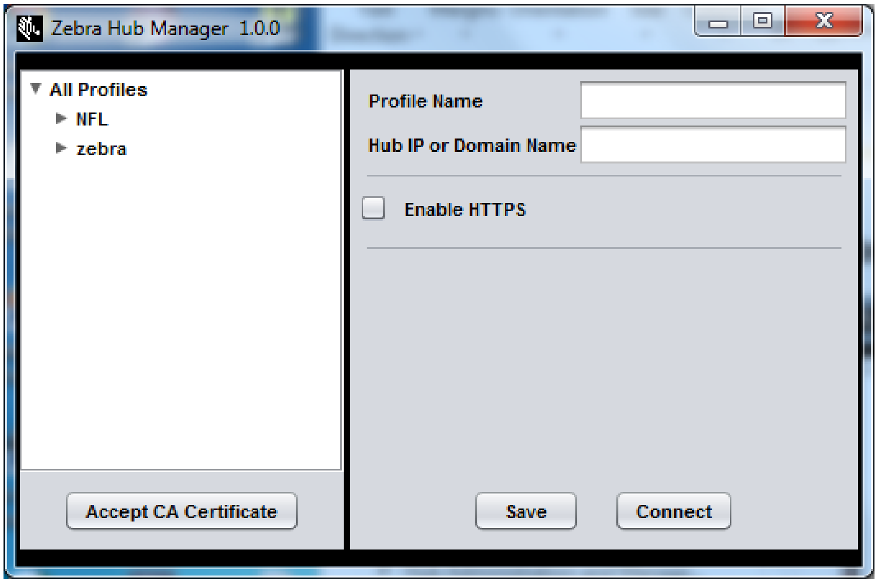
Zebra Hub Manager is a GUI application that allows the user to connect to a Dart hub and perform hub system configuration and operation supervision. Zebra Hub Manager allows user to save the hub connection parameters into a profile and manage the profile in a user friendly manner.

Please use the link below to download Zebra Hub Manager.

Zebra Hub Manager v1.0.0

The zebraHubManager.jar download has completed.

Zebra Hub Manager

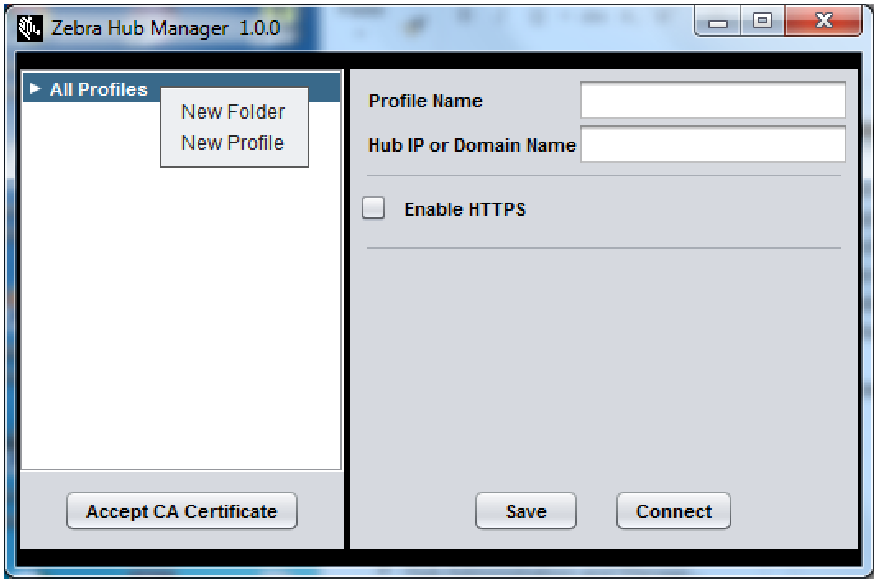


Zebra Hub Manager is a stand-alone Java application. It not only allows user to connect to hub to start the Hub Administration and Management application, and also manages hub connection parameters as profile. A profile contains a set of parameters/settings needed for connecting to a hub. A profile can be created and saved for future usage or just for one time hub access. Saved profiles are organized in folders. Moreover, Zebra Hub Manager allows user to upload trusted CA certificates, which are used to verify hub certificates when accessing hub in a secured HTTPS fashion

Creating a new folder/new profile:

1 Double click on the downloaded zebraHubManager.jar to start the application.

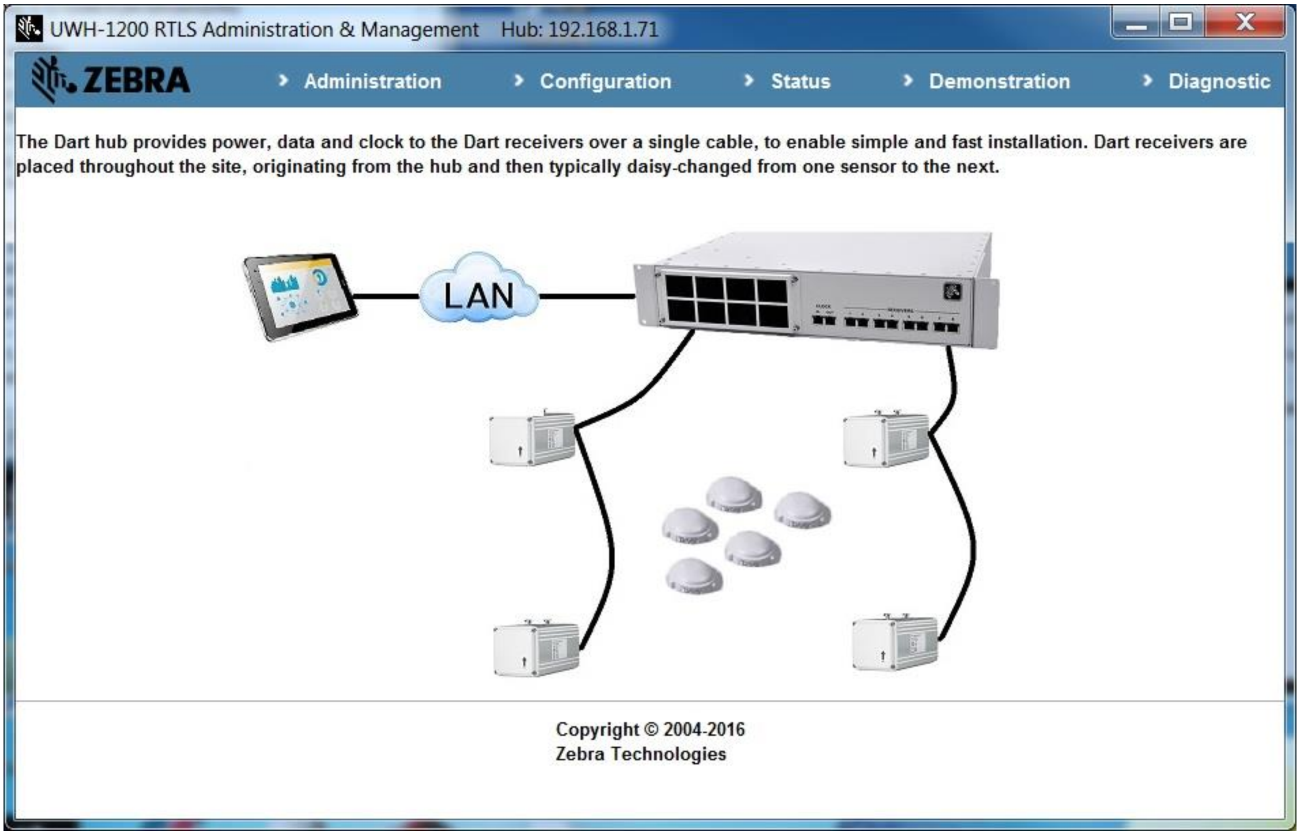
2. On the left hand side pane, click on **All Profiles**, and right click. Select either '**New Folder**' or '**New Profile**'



3. '**New Folder**' creates a new folder for saving your profiles. This way the user can organize the different hub profiles under different categories (folders). For example – Profiles for all hubs in physical location G1 can be created in a folder named 'G1'.
4. '**New Profile**' creates a new profile for the hub the user intends to access. The user needs to specify the **Profile Name** (example Lab237) and **Hub IP or Domain Name** for the hub (example 192.168.1.201). If the Hub uses secure connection, check the box '**Enable HTTPS**'. Optionally select the type of verification that needs to occur while connecting to the hub.
5. Click on **Save** to save the profile setting for the Profile Name.
6. To make changes, click on the profile Name on the left hand side panel and then edit the profile settings on the right side panel and click **Save** to save the changes.
7. To move the profile to another folder, press down left mouse button on the profile and drag and drop it into the new location.
8. To rename a folder or profile, double click on the folder/profile name and edit. After edit, press **Enter** key or just click mouse outside of the editing field.
9. To remove a profile, select the profile and right click and select **Remove**.
10. A folder can be removed only when it is empty. Click and select the folder, then right click and choose **Remove**.

Hub Administration and Management application

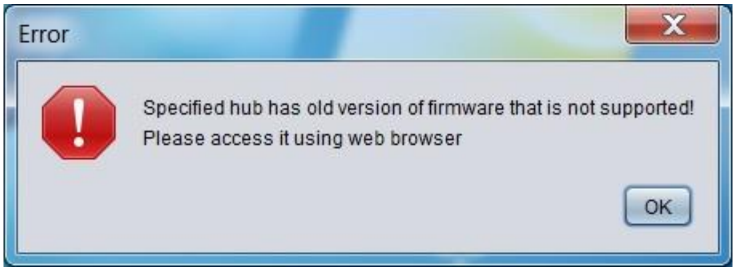
With a saved or newly created profile, click **Connect** on the Zebra Hub Manager, the hub manger retrieves and starts the Hub Administration and Management application residing on the target Hub. The look and feel of the Hub Administration and Management application hasn't changed and is similar to the Hub GUI accessed using the web browser for FW versions earlier than 5.0.0. The user can then access the Administration, Configuration, Status, Demonstration and Diagnostic pages for that particular hub, like before. The IP address of the hub is displayed on the top of the page. This helps identify which hub is being accessed in case multiple hub Administration and Management applications are open.



The Dart hub provides power, data and clock to the Dart receivers over a single cable, to enable simple and fast installation. Dart receivers are placed throughout the site, originating from the hub and then typically daisy-changed from one sensor to the next.

Copyright © 2004-2016
Zebra Technologies

If an attempt is made to access Hubs with Firmware version earlier than 5.0.0 using Zebra Hub Manager, then an error message is displayed asking the user to use the Web Browser instead of the Zebra Hub Manager to access the Hub Administration and Management GUI.



Specified hub has old version of firmware that is not supported!
Please access it using web browser

Required ports for connecting to the Dart RTLS Hub

When connecting to the Dart Hub through a network, you oftentimes need to contact your Network administrator to unblock ports for access. The following table lists the ports that are needed for all Dart RTLS functions.

Port Number	Port Use
22	Access to the Dart RTLS Hub user interface and/or output data
80	Access to the Dart RTLS Hub user interface
123	Network Time Protocol (NTP)
137	Network Basic **Input/output** System(NetBIOS) Name Service
161	Simple Network Management Protocol (SNMP)
443	Securely access to the Dart RTLS hub user interface (via HTTPS)
5110	Dart Admin, Configuration, and Diagnostic page features
5111	Dart Status page features
5117	Dart data port
5118	Dart data port. Output data is in Z-SLMF format
5119	Dart data port. Output data is in ISO format.
5120	Dart upload/download port (used for updating firmware, backup, and recalling configurations)

Software Compatibility

Dart RTLS software is compatible with following web browsers:

- Mozilla Firefox Version 38.0.5
- Internet Explorer 11 Version 11.0.9600.17801CO
- Google Chrome Version 39.0.2171.99m

Dart RTLS is compatible with the following version of Java™ Runtime Environment:

- Java™ Runtime Environment version 1.8.0_51

7 Configuring Dart RTLS

Now that your computer is connected to the Dart RTLS Hub, you can configure the Dart RTLS for tracking with one or more reference tags. Before you do this, you should familiarize yourself with setting up a single ***reference tag*** (on page 34) and then add additional reference tags as required.

To configure a single reference system:

Configure the Hub network parameters. *(on page 30)*

Establish a user-defined coordinate system. *(on page 31)*

Configure *Receiver* and reference tag positions. *(on page 32)*

Configure virtual groups *(on page 36), including boundary parameters and computation options.*

In This Section

Preparing your computer for the Dart JAVA GUI

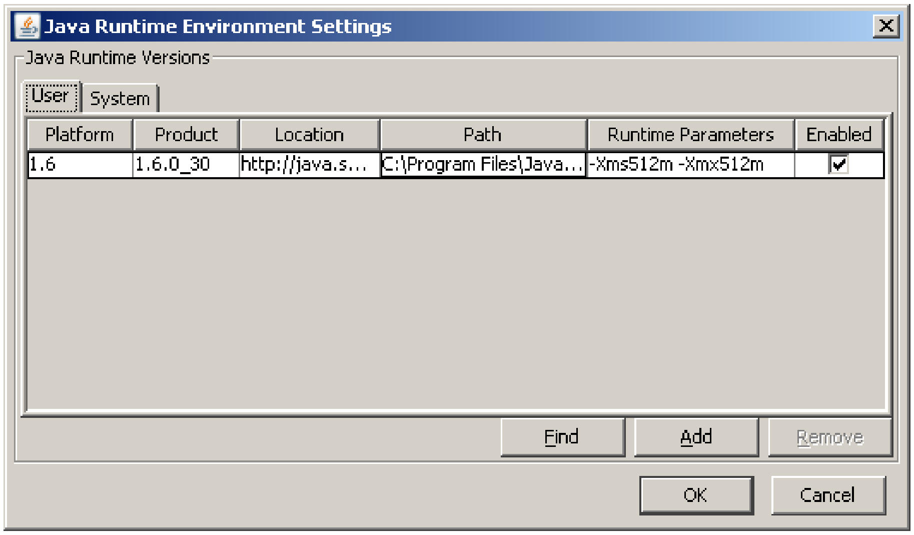
✎ For system requirements refer to page 19

Setting the JAVA virtual machine heap size for the Dart GUI

Dart hub GUI application contains Java applets running inside Java virtual machine (JVM). Whenever an applets starts, the JVM allocates a block of memory, for the applet to manage its data. The allocated heap may not be large enough to handle all operations through the Dart hub GUI. Whenever message or icon appears indicating “Out of Memory” or “Out of Java heap memory”, the user must modify the Java run-time parameters.

On windows, the Java run-time parameters can be changed using the **Java Control Panel** (accessing from **Control Panel**).

From the **Java Control Panel**, Select **Java** tab, then the **Java Runtime Environment Setting** dialog appears. Inside the table, increase the corresponding **Runtime Parameters**.



Platform	Product	Location	Path	Runtime Parameters	Enabled
1.6	1.6.0_30	http://java.s...	C:\Program Files\Java...	-Xms512m -Xmx512m	☑

Following are few options available to change heap size:

-Xms(size): set initial Java heap size.

-Xmx(size): set maximum Java heap size.

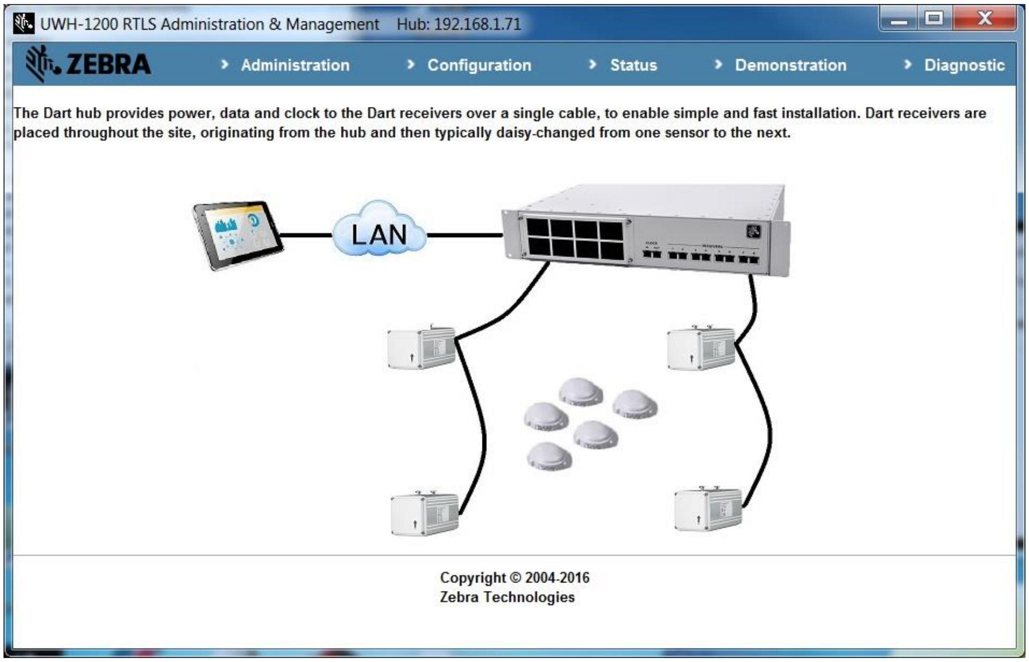
Configuring the Hub network parameters

To configure network parameters:

1 From **Zebra Hub Manager**, create a profile with hub IP address of 192.168.1.201, and use it to start **Hub Administration and Management** application on the hub

IP address 192.168.1.204 is the factory default IP address.

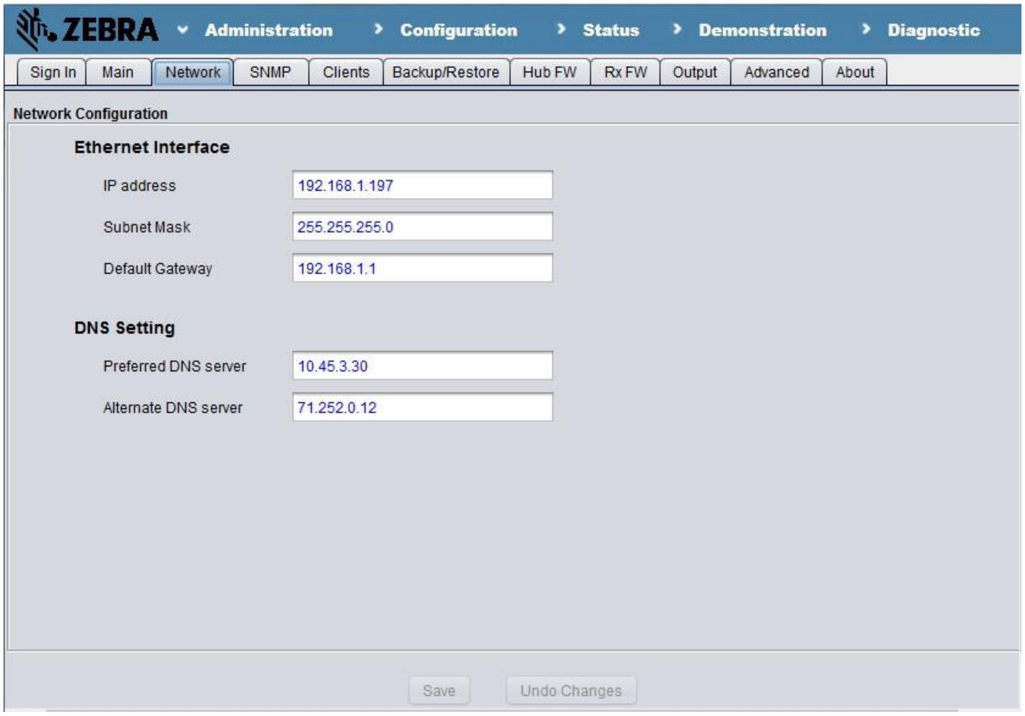
2 Click **Administration**



The Dart hub provides power, data and clock to the Dart receivers over a single cable, to enable simple and fast installation. Dart receivers are placed throughout the site, originating from the hub and then typically daisy-changed from one sensor to the next.

Copyright © 2004-2016
Zebra Technologies

3 In the **Administration** view, on the **Network** tab, modify the IP settings as needed.



Network Configuration

Ethernet Interface

IP address 192.168.1.197

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Setting

Preferred DNS server 10.45.3.30

Alternate DNS server 71.252.0.12

4 For the new IP settings to take effect, click **Save**.

Establishing a user-defined coordinate system

For tag localization, you must establish the positions of the Receivers and reference tag for the system to operate properly. This requires that you define an origin and measure the x, y, and z positions of each receiver and reference tag (in feet or meters) with respect to that origin.

To establish a user-defined coordinate system:

1. Choose an origin (0, 0, 0) point.
2. Measure the (x, y, z) coordinates of each Receiver from the (0, 0, 0) point. Make measurements to the front of the antenna.
3. Measure the (x, y, z) position of the reference tag from the (0, 0, 0) point.

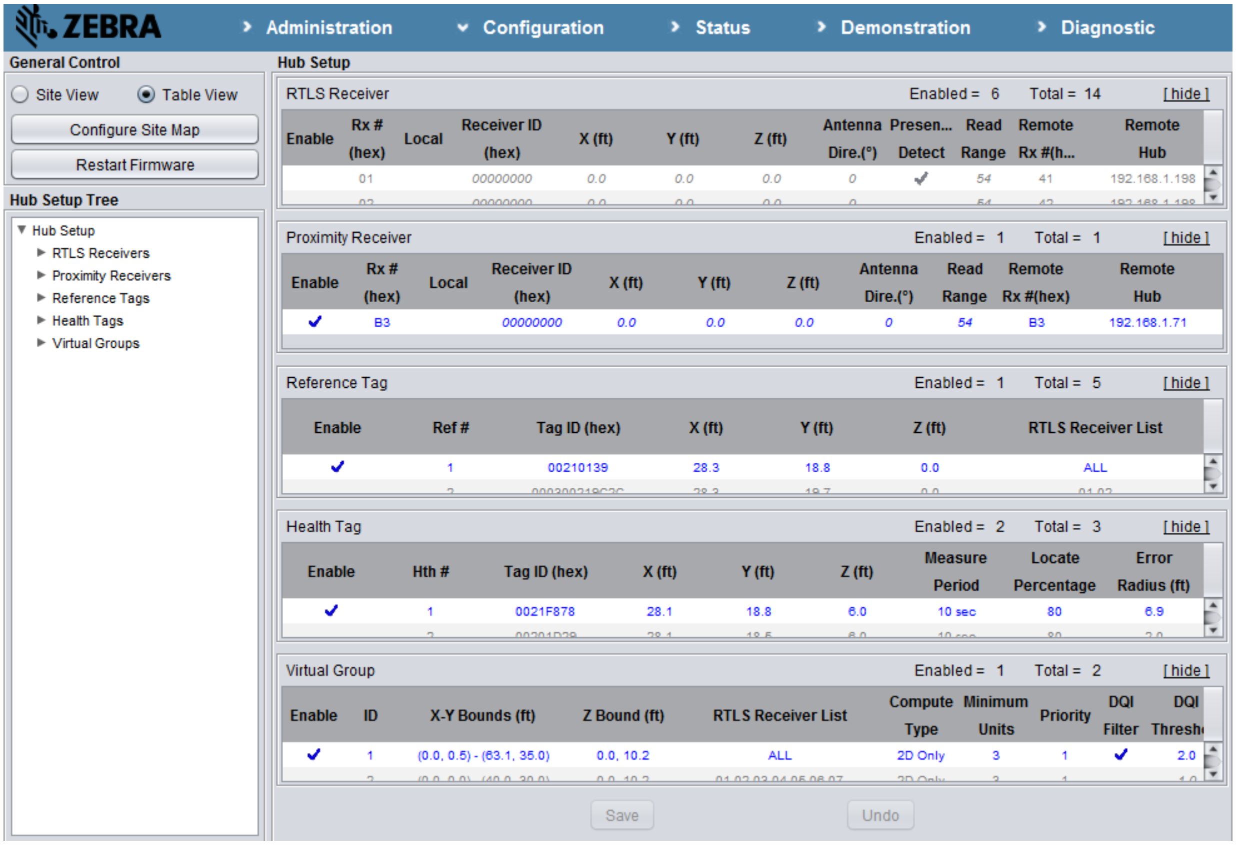
Configuring Receivers

Next, you need to define the location of each active Receiver within the system. Each receiver can be configured to be one of the following types:

- **RTLS Receivers:** Provide tag detection information to be used in locate events. When a locate event is unavailable, you can configure an RTLS Receiver to provide presence data.
- **Proximity Receivers:** Provide only presence detections. The **Read Range** setting lets you control the Sensor's range.
- **Receiver Repeaters:** A UWC-1400-R Receiver Repeater is used in applications where cable lengths greater than 1000’ are needed. The UWC_1400-R is recognized and managed by the hub but it does not detect UWB tags. On the hub, the repeater should be configured as a **Proximity Receiver**.

To configure Receivers:

1. In the **Hub Administration and Management** application, click **Configuration**.



RTLS Receiver Enabled = 6 Total = 14 [hide]

Enable	Rx # (hex)	Local	Receiver ID (hex)	X (ft)	Y (ft)	Z (ft)	Antenna Dire.(°)	Presen... Detect	Read Range	Remote Rx #(h...	Remote Hub
	01		00000000	0.0	0.0	0.0	0	✓	54	41	192.168.1.198
	02		00000000	0.0	0.0	0.0	0		54	42	192.168.1.198

Proximity Receiver Enabled = 1 Total = 1 [hide]

Enable	Rx # (hex)	Local	Receiver ID (hex)	X (ft)	Y (ft)	Z (ft)	Antenna Dire.(°)	Read Range	Remote Rx #(hex)	Remote Hub
✓	B3		00000000	0.0	0.0	0.0	0	54	B3	192.168.1.71

Reference Tag Enabled = 1 Total = 5 [hide]

Enable	Ref #	Tag ID (hex)	X (ft)	Y (ft)	Z (ft)	RTLS Receiver List
✓	1	00210139	28.3	18.8	0.0	ALL
	2	000300219C2C	28.3	19.7	0.0	01,02

Health Tag Enabled = 2 Total = 3 [hide]

Enable	Hth #	Tag ID (hex)	X (ft)	Y (ft)	Z (ft)	Measure Period	Locate Percentage	Error Radius (ft)
✓	1	0021F878	28.1	18.8	6.0	10 sec	80	6.9
	2	00201D29	28.1	18.5	6.0	10 sec	80	2.0

Virtual Group Enabled = 1 Total = 2 [hide]

Enable	ID	X-Y Bounds (ft)	Z Bound (ft)	RTLS Receiver List	Compute Type	Minimum Units	Priority	DQI Filter	DQI Thresh
✓	1	(0.0, 0.5) - (63.1, 35.0)	0.0, 10.2	ALL	2D Only	3	1	✓	2.0
	2	(0.0, 0.0) - (40.0, 30.0)	0.0, 10.2	01,02,03,04,05,06,07	2D Only	3	1		1.0

2 In the **Table View** on the **Configuration** page, under **Hub Setup,** in the **RTLS Receiver** or **Proximity Receiver** table, right-click a row and select **Add** to add a receiver (optional).

3 To modify a setting for a Receiver, double-click the respective field in the row for the Receiver that requires editing; to complete the edit, press Enter or click any other table cell.

- **Enabled:** Double-click this field to activate or deactivate a Receiver for data collection.
- **Rx # (hex):** Enter a unique hexadecimal number (01 - FF) to represent the receiver.
- **Local:** Double-click this field to indicate whether the Receiver being added is Local or not. Un-check this field as we are setting up a Remote Receiver, which is physically connected to another hub.
- **Receiver ID (hex):** Enter the 4-byte hexadecimal number found on the back label of the unit (00000010 – FFFFFFFF). Receiver ID cannot be specified for Remote Receiver.
- **X, Y, Z:** Enter the measured (x, y, z) position of the Receiver with respect to the origin (0, 0, 0) of the user-defined coordinate system. X,Y,Z cannot be specified for Remote Receiver.
- **Antenna (°):** Enter the direction (from -180° to 180°) of the receiver antenna from the direction of X axis. Antenna cannot be specified for Remote Receiver.
- **Presence Detect:** (RTLS Receivers only) Select this check box to direct the software to

output a P-packet, indicating that a tag is visible by that Receiver but position information is not available. For more information on P-packets, see ***System Output*** (on page 83).

- **Read Range:** Select a value to control the Receiver sensitivity. The value can be from 1 to 25 if in coarse range control mode, or from 1 to 54 if in fine range control mode. A Receiver is most sensitive (has the longest read range) when the **Read Range** is set to 25 for coarse range mode (or 54 for fine range mode). To set a receiver to the minimum read range, use a Read Range value of 1. For more information on read range settings and how these map to actual read ranges, see ***Appendix: Receiver read range*** (on page 125). Read Range cannot be specified for a remote receiver.
- **Remote Rx#(hex):** Enter the receiver number of the remote receiver. This should be the receiver number of the receiver as configured on the remote hub. If the Receiver is local, then Remote Rx # is 0.
- **Remote Hub:** Enter the IP address of the remote hub on which the remote receiver exists. If the Receiver is local. Then Remote Hub is 0.0.0.0

To delete a Sensor, right-click the respective row and select Remove**.**

4 Repeat Step 4 for all Receivers connected to this Hub.

5 Click **Save** for the Sensor settings to take effect.

Configuring reference tags

To compute x-y or x-y-z position, Dart RTLS requires the use of one or more reference tags. These tags help establish a common time base among the Receivers.

For a reference tag to be useful, it must be in a location that is unobstructed from at least two Receivers and not be moved from its configured position. Receivers should have an unobstructed path. If required, you can use many reference tags. However, it is generally better to use as few reference tags as possible. When deciding on how many reference tags to configure, keep these rules in mind:

- Associate each receiver with at least one reference tag.
- Associate each reference tag with more than one receiver.

The Dart Hub software uses reference tags to establish timing for computing RTLS location data. Reference tags are critical to establishing timing whenever a system restart occurs. Each of the following conditions causes a system restart:

- Any change to the setup of RTLS receivers and reference tags
- Perform a diagnostic test (**Receiver** Test , **System Test** or **Cable Test**)
- Clicking the **Restart Firmware**, **Reboot Hub**, or **Shutdown Hub** buttons
- Any power cycle to the Dart Hub
- Enabling reference tag suspension

- Updating hub FPGA firmware or receiver firmware

Once timing is established and the system is running, the reference tag is continuously monitored for presence and is used to update timing information. This monitoring is not required for accurate location data computation, but it is provided as real-time information about the status of the reference tag. If a reference tag stops transmitting, reference tag status information is available via warning messages sent out as ***D-packets*** (on page 107). These warning messages indicate that the next system restart may result in lack of location data due to insufficient reference tag information.

To configure the location of a reference tag:

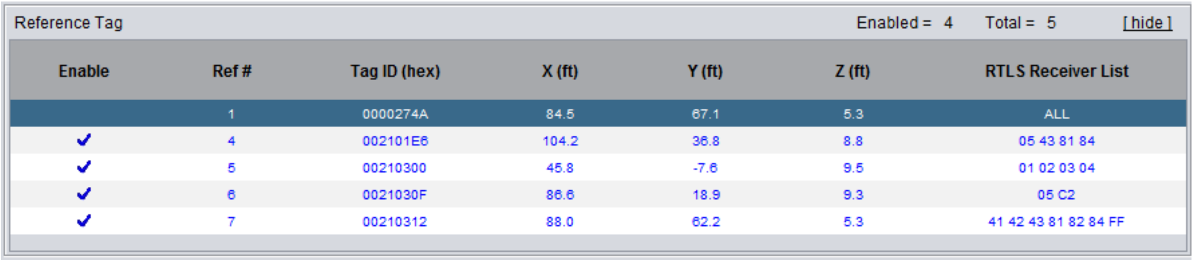
1 Start **Hub Administration and Management** application, click **Configuration**.

2 In the **Configuration** view, under **Hub Setup**, in the **Reference Tag** table, right-click a row and select **Add** to add a reference tag.

3 To modify a setting for a reference tag, double-click the respective field in the row for the reference tag that requires editing; to complete the edit, press Enter or click any other table cell:

- **Enabled:** Double-click this field to activate or deactivate a reference tag for use in calculations.
- **Ref #:** Enter a unique number (1 to 32) to represent this reference tag.
- **Tag ID (hex)**: Enter the tag ID number as shown on the barcode factory label.
- **Tag Position:** Enter the measured (x, y, z) position of the reference tag with respect to the origin (0, 0, 0) of the user-defined coordinate system.
- **RTLS Receiver List:** Enter the hexadecimal **Rx** # of each RTLS Receiver assigned in this reference group. For best results, all Receivers in the RTLS Receiver List should have a direct line of sight to the reference tag. Valid Rx # values range from 01 to FF, separated by a space.
- You can add all enabled Receivers to the reference tag group by typing **ALL** in place of a hexadecimal Receiver list.

To delete a reference tag, right-click the respective row and select Delete.



Reference Tag Enabled = 4 Total = 5 [hide]

Enable	Ref #	Tag ID (hex)	X (ft)	Y (ft)	Z (ft)	RTLS Receiver List
	1	0000274A	84.5	67.1	5.3	ALL
✓	4	002101E6	104.2	36.8	8.8	05 43 81 84
✓	5	00210300	45.8	-7.6	9.5	01 02 03 04
✓	6	0021030F	86.6	18.9	9.3	05 C2
✓	7	00210312	88.0	62.2	5.3	41 42 43 81 82 84 FF

4 Repeat Step 3 for all reference tags that this Hub uses.

5 Click **Save** for the new configuration to take effect.

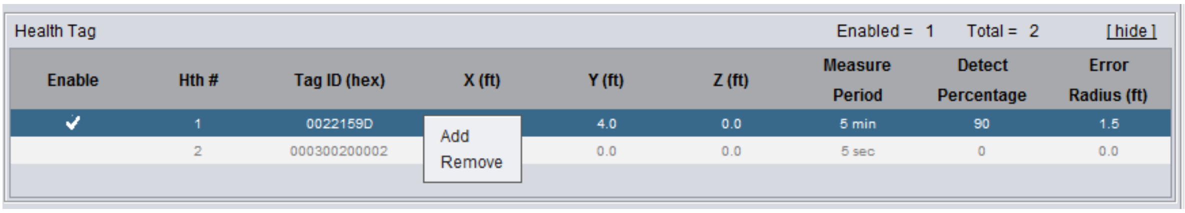
Configuring health tag

In addition to reference tags, health tags can be configured. Health tags are used to monitor system RTLS health over time.

To configure a health tag:

1 Start **Hub Administration and Management** application, click **Configuration.**

2 In the **Table** view of the **Configuration** page, find **Health Tag** configuration table



Health Tag Enabled = 1 Total = 2 [hide]

Enable	Hth #	Tag ID (hex)	X (ft)	Y (ft)	Z (ft)	Measure Period	Detect Percentage	Error Radius (ft)
✓	1	0022159D		4.0	0.0	5 min	90	1.5
	2	000300200002		0.0	0.0	5 sec	0	0.0

3 Right click on the table, from the popup menu, select **Add** or **Remove** to add a new health tag or remove an existing one**.**

4 Double click on a table cell or column of an existing health tag row to start entering corresponding health tag parameters.

- **Enable:** Double-click this field to activate or deactivate a health tag.
- **Hth #:** Enter a unique number (1 to 32) to represent this health tag.
- **Tag ID (hex)**: Enter the tag ID number as shown on the barcode factory label.
- **Tag Position:** Enter the measured (x, y, z) position of the health tag with respect to the origin (0, 0, 0) of the user-defined coordinate system.
- **Measure Period:** From the drop down list, select the time period for which the health tag is measured.
- **Detect Percentage:** Enter the locate percentage threshold. The health tag, to be considered healthy, should have the percentage of locates more than the number specified here during the **Measure Period** specified.
- **Error Radius:** Enter the error radius threshold. The health tag, to be considered healthy, should have average difference between the **Tag Position** specified and the calculated locations during the **Measure Period** specified less than the error radius specified here.

5 After editing, click **Save** to save the new UWH-1200 configuration.

To delete a health tag, right-click the respective row and select Delete.

Configuring Virtual Groups

For the Hub to be able to generate location data, you need to configure Virtual Groups among RTLS receivers. By making adjustments to these Virtual Groups, you can achieve improvements in performance and accuracy. For example, when an unobstructed view of the entire coverage area is available to all Receivers, these Receivers should belong to a single Virtual Group. However, in cases where obstructions (such as walls or large machinery) make complete coverage undependable, installing extra Receivers helps, especially when properly configured into additional Virtual Groups.

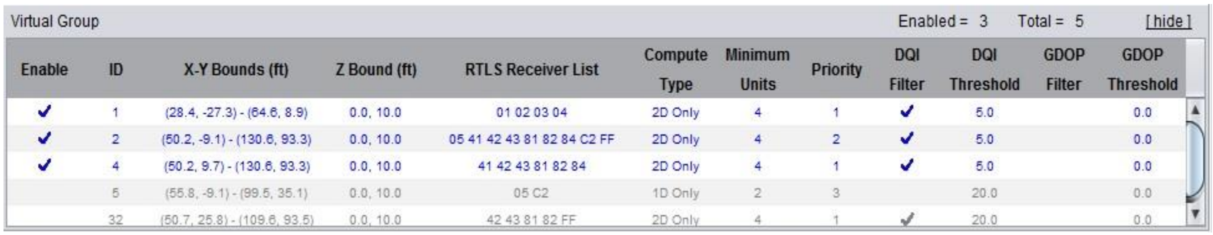
A Virtual Group is a predefined group of Receivers for which Dart RTLS calculates and reports positions. Any extra tag receptions from Receivers outside of that group do not influence the position determination from that group. Virtual Groups can overlap, and a Receiver can belong to several Virtual Groups. However, the system only performs position calculations with data received from Receivers within a common group. This keeps unreliable receptions, typically as a result of reflected signals, from harmfully influencing a position calculation.

Establishing Virtual Groups is a way of defining what Receivers are used in computing positional data; it is not related to associating Receivers with reference tags for timing.

To define Virtual Groups:

1 Start **Hub Administration and Management** application, click **Configuration**.

2 In the **Configuration** view, under **Hub Setup**, in the **Virtual Group** table, right-click a row and select **Add** to add a Virtual Group (optional).



Virtual Group Enabled = 3 Total = 5 [hide]

Enable	ID	X-Y Bounds (ft)	Z Bound (ft)	RTLS Receiver List	Compute Type	Minimum Units	Priority	DQI Filter	DQI Threshold	GDOP Filter	GDOP Threshold
✓	1	(28.4, -27.3) - (64.6, 8.9)	0.0, 10.0	01 02 03 04	2D Only	4	1	✓	5.0		0.0
✓	2	(50.2, -9.1) - (130.6, 93.3)	0.0, 10.0	05 41 42 43 81 82 84 C2 FF	2D Only	4	2	✓	5.0		0.0
✓	4	(50.2, 9.7) - (130.6, 93.3)	0.0, 10.0	41 42 43 81 82 84	2D Only	4	1	✓	5.0		0.0
	5	(55.8, -9.1) - (99.5, 35.1)	0.0, 10.0	05 C2	1D Only	2	3		20.0		0.0
	32	(50.7, 25.8) - (109.6, 93.5)	0.0, 10.0	42 43 81 82 FF	2D Only	4	1	✓	20.0		0.0

3 To modify a setting for a Virtual Group, double-click the respective field in the row for the Receiver that requires editing; to complete the edit, press Enter or click any other table cell:

- **Enabled:** Double-click this field to activate or deactivate a Virtual Group and use it to generate tag position output.
- **ID:** Enter a user-assigned ID number for association with a particular Virtual Group. Values can range from 1 to 32.
- **X-Y Bounds**, **Z Bound:** Enter the boundaries for the positional data reported by this Virtual Group. User can choose to not specify the boundary, and leave them as “none”. If the boundary is specified, Dart RTLS discards any tag data (as computed by this Virtual Group) outside of this space boundary.

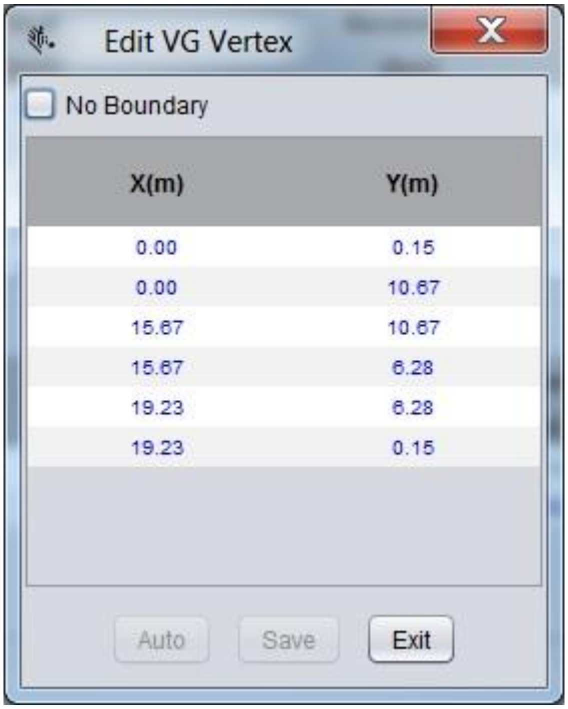
Virtual group without boundaries should only be used in system installation phase. It makes system hard to determine the scope to display in the Demonstration page and Site View of system configuration.

Double-clicking a table cell for X-Y Bounds opens the **Edit VG Vertex** dialog box. In this dialog box, do the following:

If you do not want to specify the boundary, check the **No Boundary;** otherwise, uncheck it. For a simple rectangular area, enter the two opposite vertices (that is the bottom left and top right corners) by right-clicking on the table header or table rows, and selecting **Append** or **Insert**; then click **Auto** to generate the remaining vertices of the rectangle.

Click Save to save the input X-Y bounds; then click **Exit** to close the dialog box.

For a differently shaped area, right-click on the table header or table rows, and select **Append** or **Insert**, enter the vertices, and click **Save**; then click **Exit**. To remove a vertex, right-click and select **Remove**.



□ No Boundary

X(m)	Y(m)
0.00	0.15
0.00	10.67
15.67	10.67
15.67	6.28
19.23	6.28
19.23	0.15

Double-clicking a table cell for **Z-Bound** starts editing. Enter values in the format of “min, max”. Typically, min is the smallest z coordinate value set for the Receiver positions, and max is the largest z coordinate value set for the Receiver positions.

- **RTLS Receiver List:** Enter the Rx #, range from 01 to FF, of each **Receiver** to be associated with the Virtual Group, separated by a space. Alternatively, to add all enabled Receivers to the virtual group, type **ALL** in the **RTLS Receiver List** field.
- **Compute Type:** Select one of the following compute types to be used for computing information:

  1D Only—Select if you want the system to perform 1-D calculations when two Receivers detect the tag transmission. 1D-Only virtual groups permit only two RTLS Receivers.

  2D Only—Select if you want the system to perform 2-D calculations when three or more RTLS Receivers detect the tag transmission. For accurate 2D calculations, the entire X-Y space to track must be surrounded by receivers and the X-Y distances need to be relatively equivalent.

  3D Only—Select if you want the system to perform 3-D calculations when four or more RTLS Receivers detect the tag transmission. For accurate 3D calculations, the entire X-Y-

Z space to track must be surrounded by receivers and the X-Y-Z distances need to be relatively equivalent. In most installations, it is not practical to install receivers in positions where the X-Y-Z criteria yield accurate results.

1D and 2D—Select if you want the system to perform 2-D calculations when three or more RTLS Receivers detect the tag transmission; alternatively, it provides 1D position data when two RTLS Receivers detect the tag transmission.

2D and 3D—Select if you want the system to perform 3-D calculations when four or more RTLS Receivers detect the tag transmission; alternatively, it provides 2-D position data whenever three RTLS Receivers detect the tag transmission.

- **Minimum Units:** Select the minimum number of RTLS Receivers that must detect a specific tag transmission for location computation. Sometimes, requiring more Receivers within a given Virtual Group to have received a tag transmission before computing the tag position can enhance accuracy. If **Compute Type** is set to 1D, 1D/2D, or 2D/3D, this field is unavailable for editing.

  The following list specifies the minimum number of Receivers required per **Compute Type**:

  - 1D and 2D data: 2
  - 2D and 3D data: 3
  - 1D data only: 2 (minimum and maximum)
  - 2D data only: 3 or more
  - 3D data only: 4 or more

- **Priority:** Select the priority of this Virtual Group for arbitrating between tag data positions that are calculated by two or more Virtual Groups. The group with the highest priority for a given successful data computation generates output. When a tag transmission is received in more than one Virtual Group, the hub software will generate, in addition to a location result for each group, an estimate of the time of that transmission. Rather than output a location result for each VG with the same priority, the hub software will compare the time estimates and only select for output the result from the VG with the earliest transmission time. Since this result is based on data from the most direct signal path, it is the best estimate of location. This selection is only possible when the various VGs are properly connected with overlapping and functioning reference groups.

  For example:

  Example 1—Groups having unique priorities. This causes the highest priority group (lowest numerical value) with a successful data computation to output position data.

  Example 2—All groups set with equal priority. This causes all successful data computations from all enabled virtual groups are under further arbitration to generate data output.

Example 3—Groups having a mixture of equal and unique priorities. For example, there could be four Virtual Groups with the following results from a given tag transmission:

Virtual Group 1 with priority 1 does not compute data successfully.
Virtual Group 2 with priority 2 does compute data successfully.
Virtual Group 3 with priority 2 does compute data successfully.
Virtual Group 4 with priority 3 does compute data successfully.

In this case, Virtual Groups 2 and 3 have equal priority and have higher priority than other groups with successful computations. Therefore, the computation result from both group 2 and group 3 are evaluated by the hub to determine which VG output had the earliest transmission time. The VG with the earliest transmission time is sent as output from the hub. Filtering output-based virtual group priorities is considered an advanced feature requiring experimentation.

Note : In FW version 5.0.0 and up, to optimize calculation time, the lower priority VGs are calculated only if high priority VG do not yield locates. In Example 3, if VG 2 and 3 computes data successfully, data from VG 4 is not computed.

- **DQI Filter:** Double-click this field to turn on or off the suppression of tag location data with quality indicators (DQI) greater than the value specified in the **DQI Threshold** field.
- **DQI Threshold:** Specify the value beyond which tag location data will be suppressed. Larger DQI values generally indicate a larger data error, or poorer accuracy in the position measurement. In an ideal world without measurement errors, the DQI value would be zero.
- **GDOP Filter:** Geometric Dilution of Precision (GDOP) is used to quantify the location accuracy of each tag blink based on the geometry of the receivers detecting the tag blink and the calculated tag location. Double-click this field to turn on or off the suppression of tag location data with Geometric Dilution of Precision (GDOP) greater than the value specified in the **GDOP Threshold** field.
- **GDOP Threshold:** Specify the value beyond which tag location data will be suppressed. Larger GDOP value generally indicates lower reliability on the position measurement (indicates poor geometry). Normally, a location calculated with GDOP value above 2.0 is not that trustable. GDOP filter is a site specific setting. In theory, GDOP threshold in the range of 1.0 to 1.4 is a good setting for a well-designed deployment.

Filtering output based on DQI or GDOP values is considered an advanced feature requiring experimentation; initial and possibly most installations should avoid using this feature.
The DQI Filter, DQI Threshold, GDOP filter and GDOP threshold options only apply to successful data computations. Data computation is successful when a computed position that is based on a tag event satisfies the group boundary constraints and computation options described above.

To delete a virtual group, right-click the respective row and select **Remove**

4. Repeat Step 3 for every Virtual Group to be used by this Hub.
5. Click **Save** for the Virtual Group configuration to take effect.

8 Configuring output control

By default, the Dart RTLS Hub provides a data output stream in various formats

For information on available output data formats, see ***System output*** (on page 83)

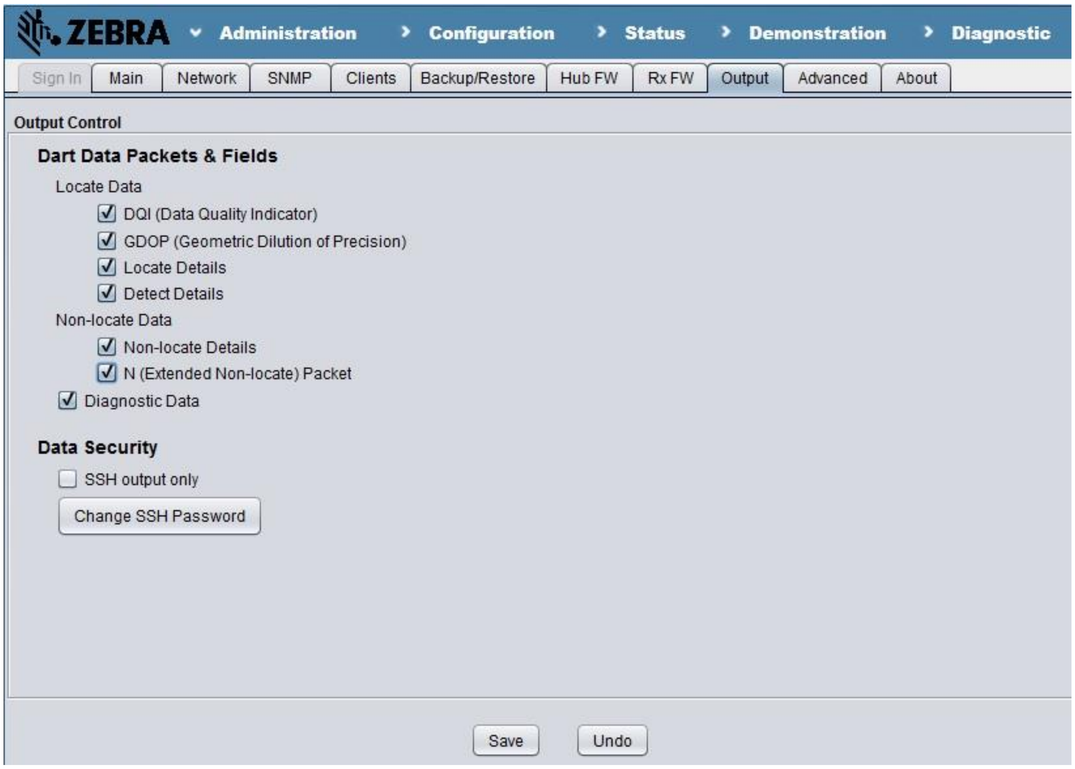
You can modify the data output from the Hub to:

- Enable output of diagnostic messages (D-packets) from the Hub.
- Indicate the quality of data provided from the Hub for Locate and Non-locate data.

To configure output control:

1 Start **Hub Administration and Management** application, click **Administration**.

2 In the **Administration** view, on **Output** tab, select the desired check boxes to enable output data fields:



Output Control

Dart Data Packets & Fields

Locate Data

☑ DQI (Data Quality Indicator)

☑ GDOP (Geometric Dilution of Precision)

☑ Locate Details

☑ Detect Details

Non-locate Data

☑ Non-locate Details

☑ N (Extended Non-locate) Packet

☑ Diagnostic Data

Data Security

☐ SSH output only

- **Diagnostic Data.** Select the check box to include D-packets in the corresponding output stream. D-packets help diagnose problems encountered during both installation and normal operation. Dart RTLS sends D-packets during system initialization, after each firmware restart, or after saving the configuration. For non-critical errors or events, the system sends the corresponding D-packet only once each time an event or warning condition occurs. For critical system errors, the system sends the D-packets continuously until the error is cleared.

Dart Output Stream

With D-packets, the Dart data output stream has the following format:

```
D,<ID>,<X>,<Y>,<Z>,<battery>,<timestamp>,<DpacketID>,‘readable
info’<LF>
```

- **Locate Data**
  - **Data Quality Indicator (DQI).** Select to quantify the quality of the position data that the

    Hub calculates. The Dart RTLS system calculates the DQI through a minimization process during location computations. DQI data is only meaningful for 2D and 3D data computations where more receivers are used in the computation than required for minimum calculation. Otherwise (for presence or 1D data), the field displays an asterisk in the output.

    Dart Output Stream

    With DQIs, the Dart output stream has the following format for location messages:

    ```
    <Data Header>,<tag ID>,<X>,<Y>,<Z>,<battery>,<timestamp>,
    <unit>,<DQI><LF>
    ```

    If a DQI is not available, this field contains an asterisk (*).

For a 2-D (T-packet) or 3-D (R-packet) DQI value to be meaningful, the system must have additional Receiver information available when computing tag locations. In general, 2-D computations require at least three Receivers to detect the tag transmission. For a meaningful DQI in a 2-D computation, at least four Receivers must detect the tag transmission. To guarantee meaningful DQIs, you can increase the minimum number of Receivers within a virtual computation to four (or more) for a 2-D computation.

  - **Geometric Dilution of Precision (GDOP).** Select to include GDOP value of calculated tag location. GDOP is calculated based on the output tag location and configured location of involved receivers. GDOP value is only meaningful for 2D and 3D data computation. Otherwise (for presence and 1D data), the field displays an asterisk in the output.

    Dart Output Stream

    With GDOP, the Dart output stream has the following format for location messages:

    ```
    <Data Header>,<tag ID>,<X>,<Y>,<Z>,<battery>,<timestamp>,
    <unit>,<GDOP><LF>
    ```

  - **Locate Details.** Select to display Receivers used in computing location data. This is helpful when assessing why location data is different than expected. It can be useful in identifying undesirable reflected signals that may be causing Receivers to contribute to location computations.

Dart Output Stream

With RTLS data information, the Dart data output stream has the location data message in following format:

```
<Data Header>,<tag ID>,<X>,<Y>,<Z>,<battery>,<timestamp>,
<unit>,<Locate-Details><LF>
```

- **Detect Details.** Select to include detect details in the locate. With this enabled, locates will now contain details about RTLS receivers that detected the blink (***Proximity receivers are excluded from consideration here)*** and receivers that were pruned/pre-pruned.

  With additional detect details, the data output has the format Hrr[Pvv][Rvv] where

  - Hrr : indicates receiver with receiver number rr detected the tag blink
  - Pxx : indicates receiver rr was pre-pruned during tag location calculation in virtual group xx. Pxx may not appear if the receiver was not pre-pruned in any virtual group; it might appear multiple times if the receiver was pre-pruned in more than one virtual group.
  - Ryy: indicates receiver rr was pruned during tag location calculation in virtual group yy. Ryy may not appear if pruning is turned off or if receiver was not pruned in any virtual group; it might appear multiple times if the receiver was pruned in more than one virtual group.

- **Non Locate Data:**

  - **Non-locate Details.** Select to display detail information for events where location data is not available. This is helpful when assessing why location data is unavailable for a particular tag event.

    For a description of the Non-locate details the Dart RTLS system generates, see ***Non-locate Details*** (on page 85).

    Dart Output Stream

    With P-data information, the Dart data output stream has the presence data message in following format:

    ```
    P,<tag ID>,<X>,<Y>,<Z>,<battery>,<timestamp>,<receiver #>,<Non-
    locate-Details><LF>
    ```

  - **N (Extended Non-locate) packets.** Enable to get ‘N’ packets that contain extended information for a ‘P’ packet. ‘N’ packets facilitate getting more information for a ‘P’ packet by including the detect details. The format of the ‘N’ packet is as follows:

    ```
    N,<tag #>,0.0,0.0,0.0,<battery>,<timestamp>,00,<non-locate
    details>,<detect details><LF>
    ```

When ‘N’ packets are enabled, non-locates generate ‘N’ packets ***instead*** of ‘P’ packets.

3 Click **Save**.

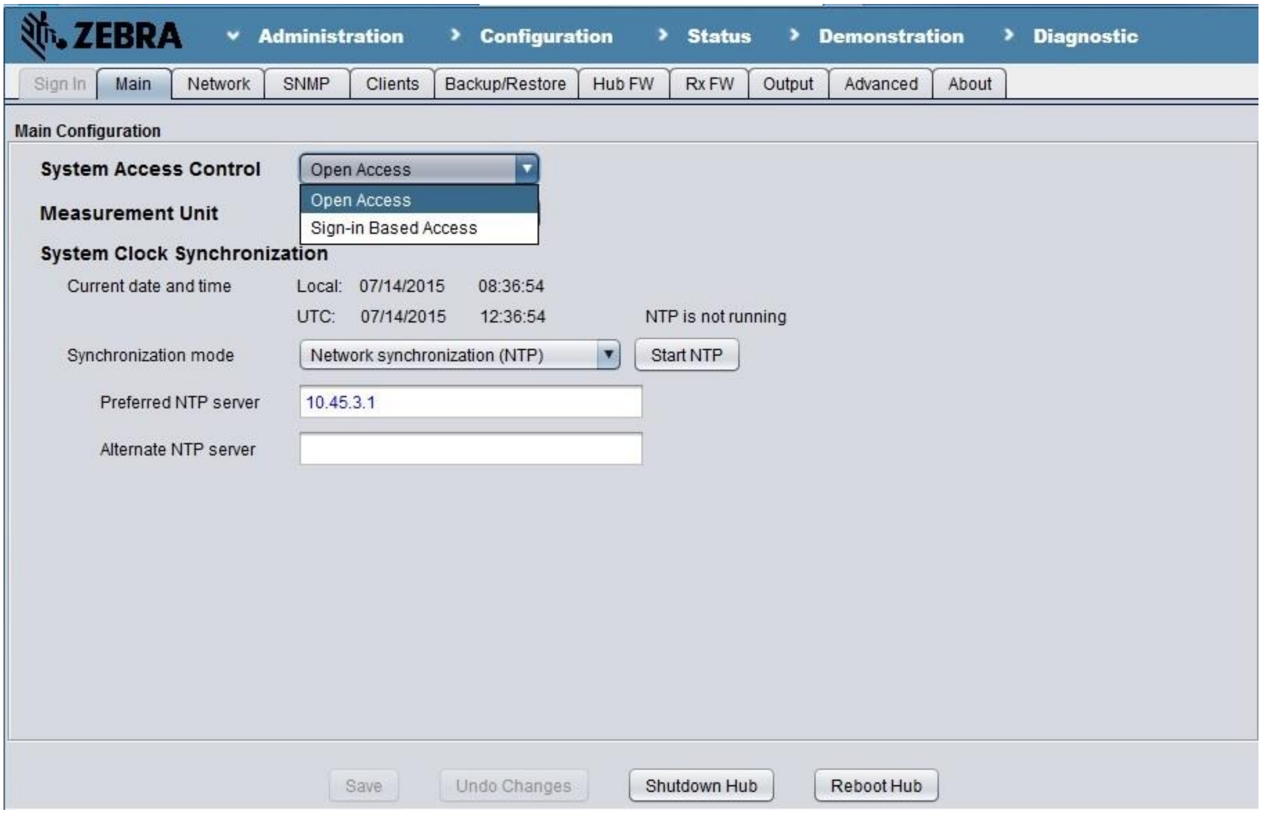
9 Hub administration

You can use the **Hub Administration and Management** application to administer the Dart RTLS Hub.

In This Section

Access protection on the Hub

UWH1200 Hub provides optional role based access control and keeps a log of events with details on hub access and configuration changes. The access control setting on the ‘Main’ tab lets the user select if Open Access is preferred or Sign-in Based Access is preferred. With Open Access, anyone accessing the hub will have administrator access and only one user access is allowed at a time. If Sign-In based access is selected, the hub provides a new security tab ‘Sign In’, which requires the user to log in before any changes can be made to the hub through the user interface of the hub. In this mode, at any time, up to ONE administrator/operator connection can be established via successful user login and multiple guest connections can be established.



Main Configuration

System Access Control: Open Access
- Open Access
- Sign-in Based Access

Measurement Unit

System Clock Synchronization

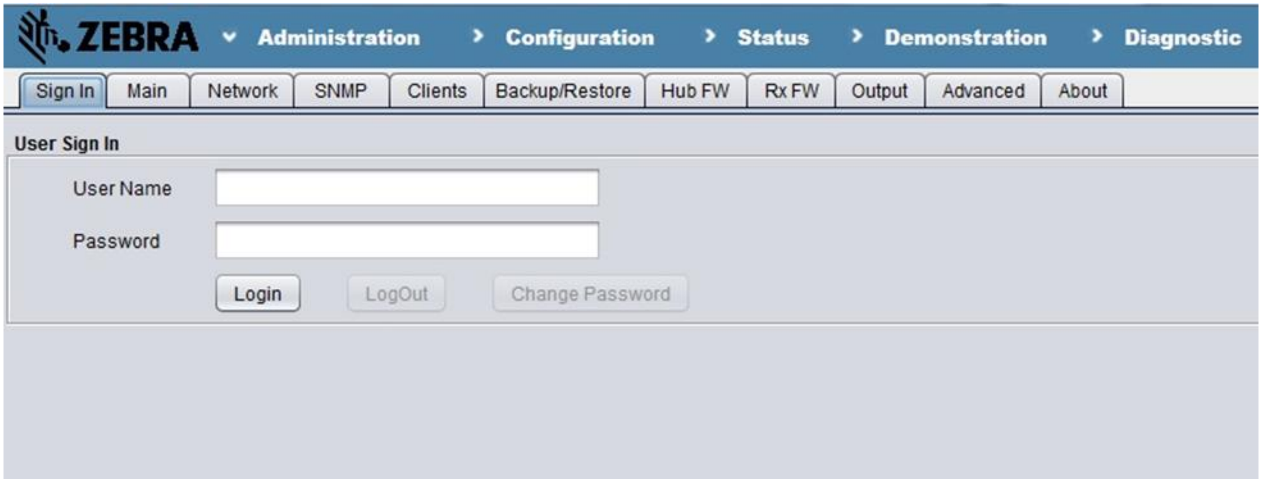
Current date and time Local: 07/14/2015 08:36:54
UTC: 07/14/2015 12:36:54 NTP is not running

Synchronization mode: Network synchronization (NTP)

Preferred NTP server: 10.45.3.1

Alternate NTP server:

Hub Log-In



The hub is shipped with the following default user name and password –

Username : admin
Password : Admin1234

Both user name and password are case sensitive. A valid password should have a minimum length of 8 characters and should contain at least 1 uppercase character, 1 lowercase character and 1 number.

Log-In Rules

The following rules apply for log in/log out for administrator and operator roles

- Upon inactivity of more than 5 minutes, the user is automatically logged out and trying to access any GUI features will force the user to re-login.
- While the user is logged in and remains active, if the **Hub Administration and Management** application is closed by accident, the user can reconnect to the hub within 15 seconds, without being required to re-login. In other words, user login expires 15 seconds after disconnecting from the hub.
- Once logged in, unless explicitly log out or wait for log in expired, no other user can access the hub as an administrator or an operator. The same user cannot establish another connection to the hub with same credentials using the same or a different computer.

Roles and Permissions

Access to the hub is granted for users in 3 different roles – as an administrator, as an operator or as a guest. When the user initially opens the hub GUI, the GUI can be viewed as a guest, upon logging in with a valid user name and password, the GUI can be accessed in operator or administrator’s role. Once logged in, the user can navigate across the different web pages (administration, configuration, status etc.) without having to log in again.

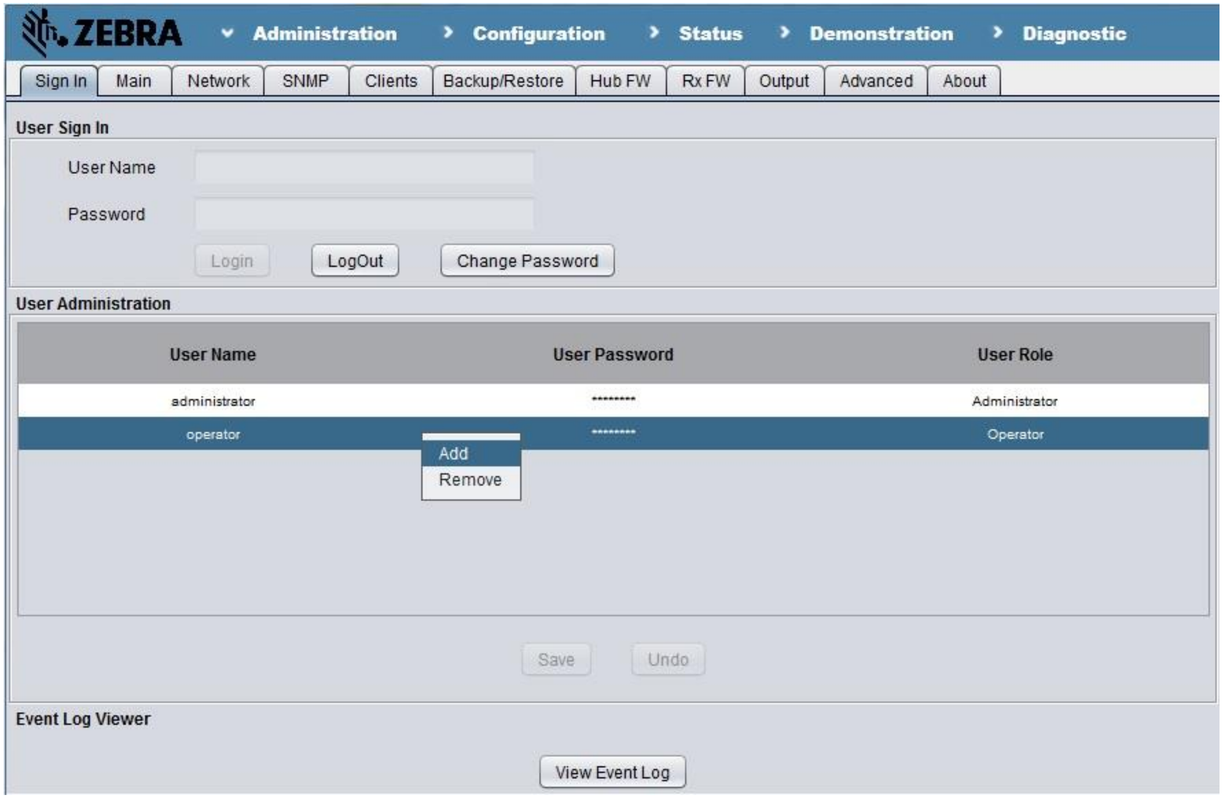
- **Administrator -** Administrator has full access to the hubs configuration and settings. Administrator can create users and assign roles to the users. Administrator can also change passwords for the users and delete the user accounts.
- **Operator –** Operator has access to all the features on the hub GUI except creating or modifying user accounts. Operator also cannot change hub network settings (NTP, Network, SNMP). Operator can change the password of his/her own account.
- **Guest –** Guest can only view and cannot modify configuration/ settings on the hub GUI.

	Administrator	Operator	Guest
Configuration change	√	√	×
System Access control setting change	√	×	×
General Admin	√	√	×
Network admin(NTP, Network, SNMP)	√	×	×
Status	√	√	√
Diagnostics	√	√	×
New user account	√	×	×
Any Password Reset	√	×	×
User Password Reset	√	√	×
Configuration and Settings View	√	√	√
Event log view	√	x	x

Administrator Access

To create new user or change role and password:

1. Start **Hub Administration and Management** application, click **Administration**.
2. Log in as administrator, under **Sign In** tab using the default username and password provided. Click on **Login.**
3. Under **User Administration**, right click a row and select **Add** to add a user (optional).
4. Click on the newly created row under **User Name** and type in the user name desired.
5. Create a password adhering to the rule mentioned above, under **User Password.**
6. Finally choose what role the new user should have – **Administrator** or **Operato**r. Click **Save** to create the new user. Click **Undo** (before clicking Save) to remove the entry just added
7. To delete a user account, right click a row and select **Remove** to remove that user. Click **Save.**



User Name	User Password	User Role
administrator	********	Administrator
operator	********	Operator

Operator access

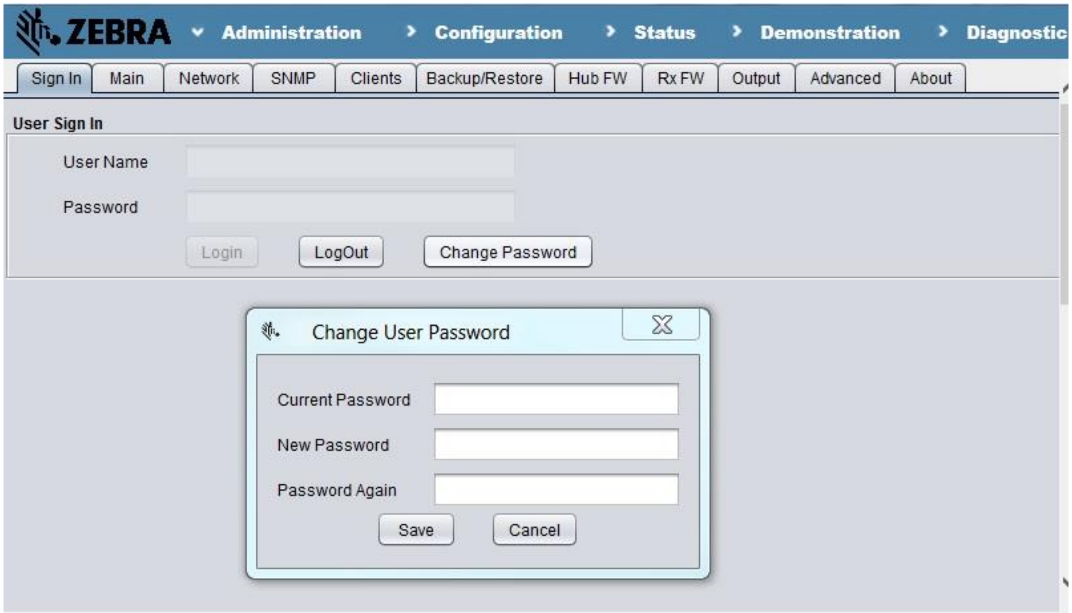
To log-in and change password

1 Start **Hub Administration and Management** application, click **Administration**

2 Log in as operator, under **Sign In** tab, using the username and password provided by your administrator. Click on **Login**.

3 Click **Change Password**. Enter the **Current Password** and **New Password** (twice) to change the password for the operator account. Click **Save**.

4 For security, click **LogOut** after the session is done.

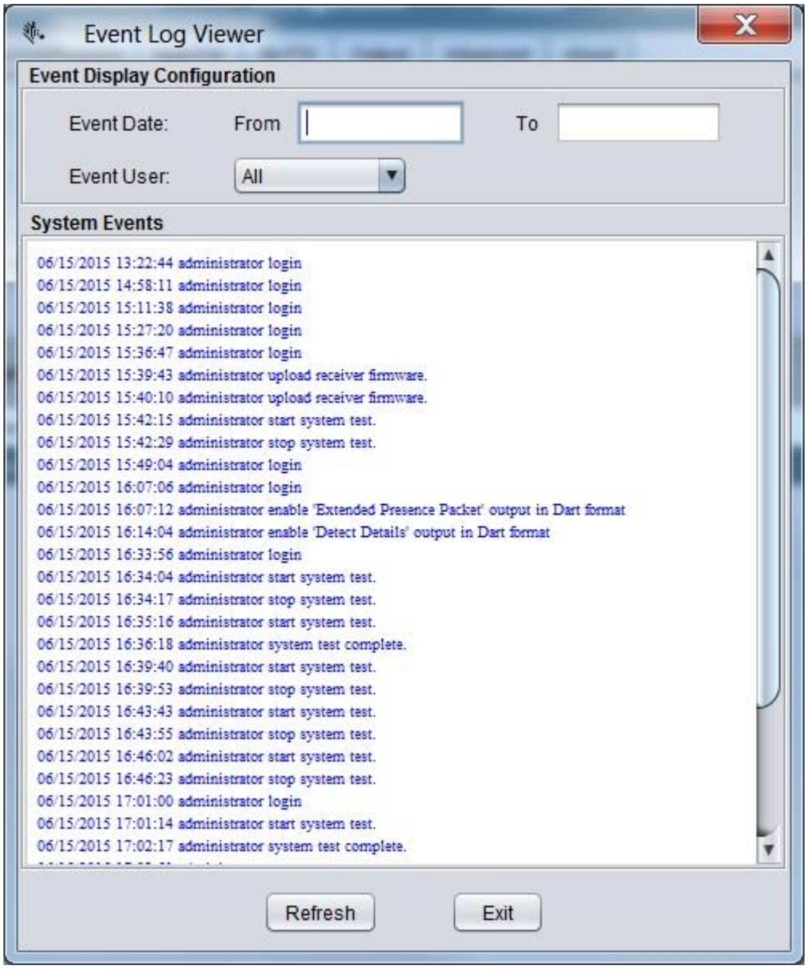


Event Log

The hub supports event logging on hub user access and configuration changes. Event Log can be viewed only when **System Access Control** on the Main Tab is set to '**Sign-In Based Access**' and user is logged in as an Administrator. The events are logged for the following actions

- User log in/log out,
- User account create/delete or password change.
- Changes on Administration page
- Changes on Configuration page
- Action or setting changes on diagnostic page.
- Uploads of hub firmware, hub FPGA firmware or receiver firmware
- Hubsitedata file push from SystemBuilder.

The Event log entries can be filtered based on Event User or Event Date. Note – the log is maintained across firmware updates to the hub.



```
06/15/2015 13:22:44 administrator login
06/15/2015 14:58:11 administrator login
06/15/2015 15:11:38 administrator login
06/15/2015 15:27:20 administrator login
06/15/2015 15:36:47 administrator login
06/15/2015 15:39:43 administrator upload receiver firmware.
06/15/2015 15:40:10 administrator upload receiver firmware.
06/15/2015 15:42:15 administrator start system test.
06/15/2015 15:42:29 administrator stop system test.
06/15/2015 15:49:04 administrator login
06/15/2015 16:07:06 administrator login
06/15/2015 16:07:12 administrator enable 'Extended Presence Packet' output in Dart format
06/15/2015 16:14:04 administrator enable 'Detect Details' output in Dart format
06/15/2015 16:33:56 administrator login
06/15/2015 16:34:04 administrator start system test.
06/15/2015 16:34:17 administrator stop system test.
06/15/2015 16:35:16 administrator start system test.
06/15/2015 16:36:18 administrator system test complete.
06/15/2015 16:39:40 administrator start system test.
06/15/2015 16:39:53 administrator stop system test.
06/15/2015 16:43:43 administrator start system test.
06/15/2015 16:43:55 administrator stop system test.
06/15/2015 16:46:02 administrator start system test.
06/15/2015 16:46:23 administrator stop system test.
06/15/2015 17:01:00 administrator login
06/15/2015 17:01:14 administrator start system test.
06/15/2015 17:02:17 administrator system test complete.
```

Uploading certificates to Zebra Hub

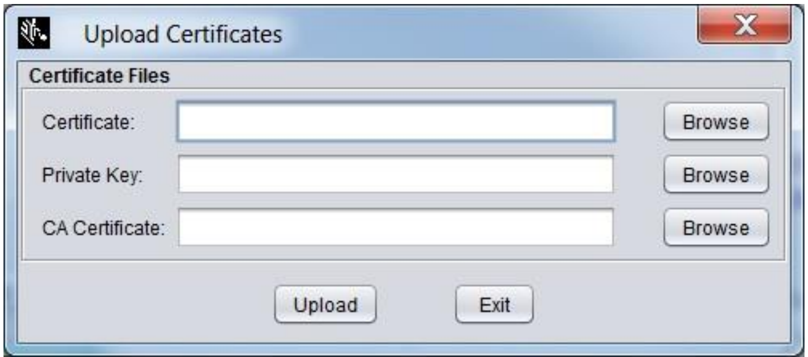
1 Uploading the certificate to the hub, the user may need to covert received certificate into three files:

- Hub certificate in PEM format
- CA certificate contain the whole certificate path from hub certificate issuer to a trusted CA in PEM format
- unencrypted private key in PEM format

2 Start **Hub Administration and Management** application, click **Administration**, then enter **Sign In** tab.

3 If the hub is configured to use **Open Access** mode, Select **Sign In Based Access** in the **System Access Control** in **Main** tab, and click **Save** to enable and enter **Sign In** tab.

4 Click **Upload Certificates.**



5 Browse or input the path to three certificate files as list in step 1**.**

6 Click **Upload.**

Defining the measurement units for coordinates

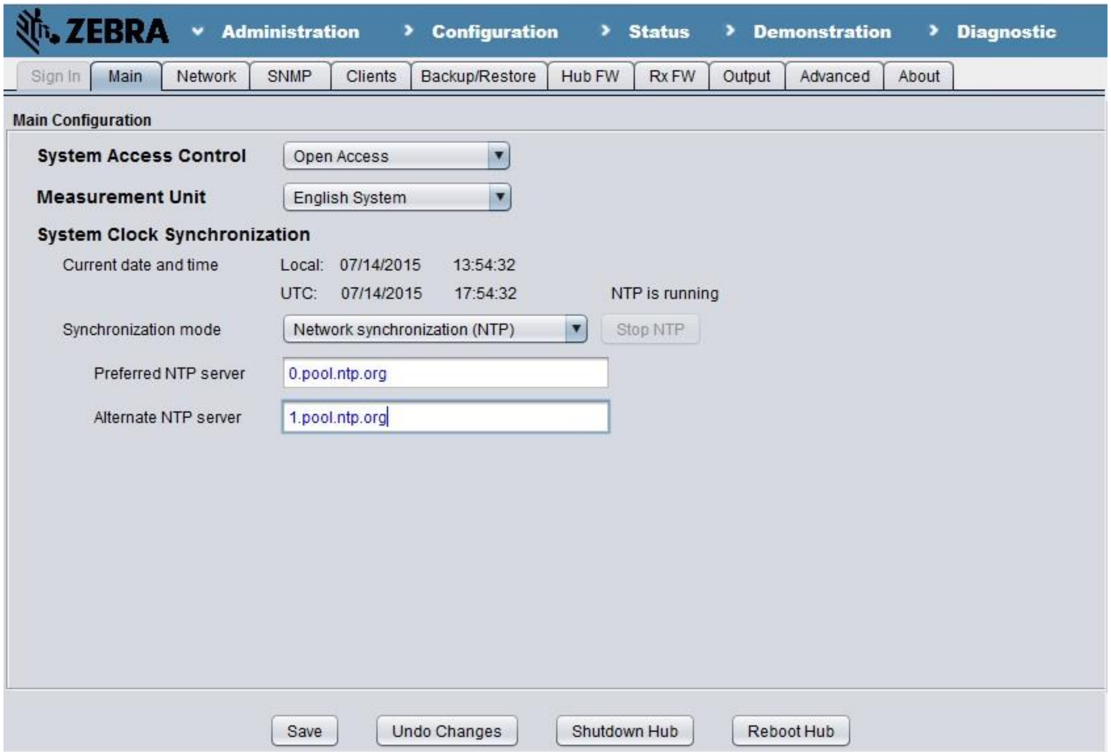
You can specify whether Dart RTLS should store configuration information in feet or meters.

To define the measurement unit system:

1 Start **Hub Administration and Management** application, click **Administration**.

2 In the **Administration** view, on the **Main** tab, under **Measurement Unit**, select **English System** to display information in feet or **Metric System** to display information in meters.

3 Click **Save**.



Main Configuration

System Access Control: Open Access

Measurement Unit: English System

System Clock Synchronization

Current date and time
Local: 07/14/2015 13:54:32
UTC: 07/14/2015 17:54:32
NTP is running

Synchronization mode: Network synchronization (NTP)

Preferred NTP server: 0.pool.ntp.org

Alternate NTP server: 1.pool.ntp.org

Synchronizing the Dart system clock

You can set the Dart system clock by:

- Manually entering time and date
- Synchronizing with the host computer
- Network Time Protocol (NTP)

The NTP daemon synchronizes the system time with a user-specified NTP server. For more information about NTP and a list of public time servers, check the NTP Website at http://www.ntp.org.

Proper operation of the NTP System Clock Synchronization feature requires that you specify the DNS setting. Check with your system administrator to determine what DNS setting to use for your network.

To synchronize the Dart system clock to NTP:

1 Start **Hub Administration and Management** application, click **Administration**.

2 In the **Administration** view, on the **Main** tab, under **System Clock Synchronization**, from the **Synchronization mode** list, select **Network synchronization (NTP)**.

3 In the **Preferred NTP server** and **Alternate NTP server** fields, enter the IP address or URL of the respective servers.

4 Click **Save** for the new setting to take effect.

To synchronize the Dart system to a local computer:

1 Start **Hub Administration and Management** application, click **Administration**.

2 In the **Administration** view, on the **Main** tab, under **System Clock Synchronization**, from the **Synchronization mode** list, select **Local host's date and time**.

3 Click **Save**.

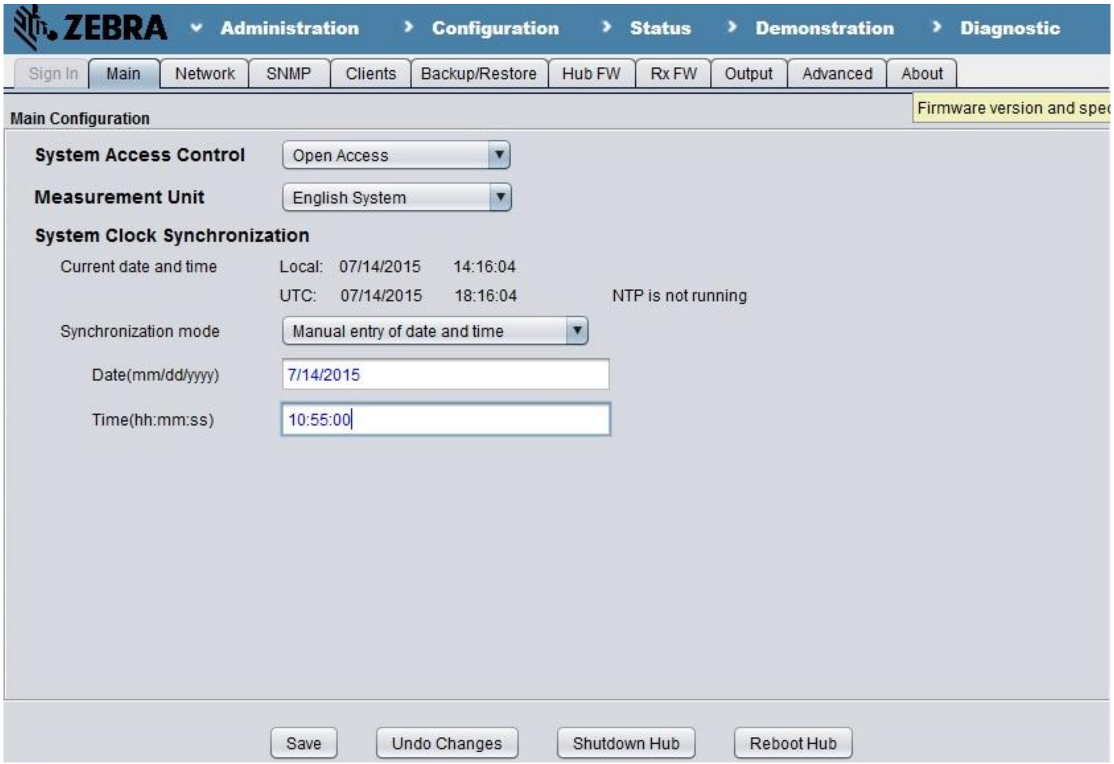
To manually enter a time and date for the Dart system:

1 Start **Hub Administration and Management** application, click **Administration**.

2 In the **Administration** view, on the **Main** tab, under **System Clock Synchronization**, from the **Synchronization mode** list, select **Manual Entry of Date and Time**.

3 Enter the required date and time.

4 Click **Save**.



Main Configuration

System Access Control: Open Access

Measurement Unit: English System

System Clock Synchronization

Current date and time — Local: 07/14/2015 14:16:04

UTC: 07/14/2015 18:16:04 — NTP is not running

Synchronization mode: Manual entry of date and time

Date(mm/dd/yyyy): 7/14/2015

Time(hh:mm:ss): 10:55:00

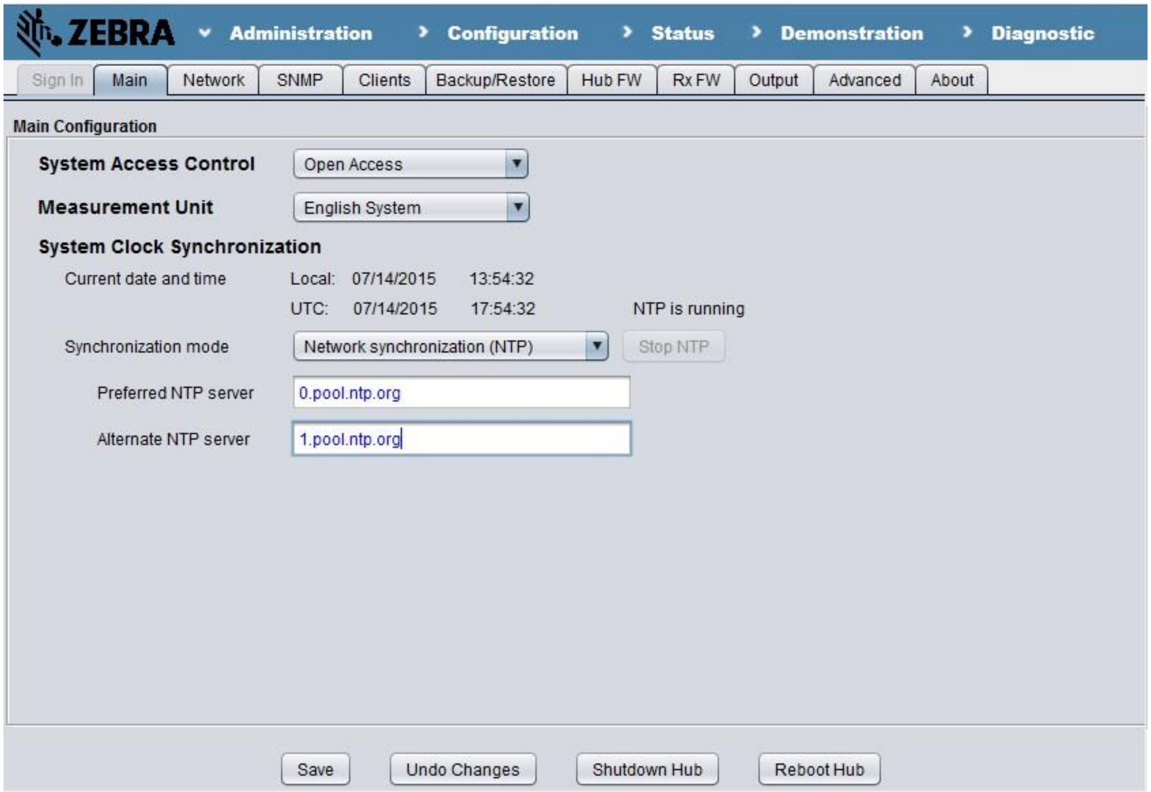
Shutting down the Hub processor

Before you turn off power to the Dart RTLS Hub, Zebra recommends that you shut down the Hub processing software.

To shut down the Hub processing software:

1 Start **Hub Administration and Management** application, click **Administration**.

2 In the **Administration** view, on the **Main** tab, click **Shutdown Hub**.



Main Configuration

System Access Control: Open Access

Measurement Unit: English System

System Clock Synchronization

Current date and time — Local: 07/14/2015 13:54:32

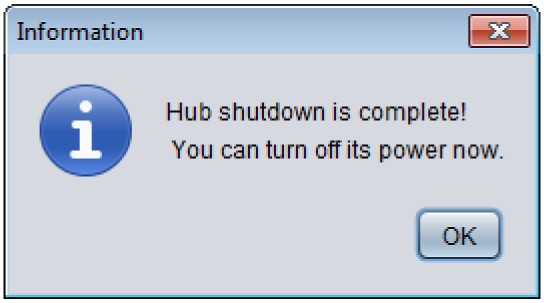
UTC: 07/14/2015 17:54:32 NTP is running

Synchronization mode: Network synchronization (NTP)

Preferred NTP server: 0.pool.ntp.org

Alternate NTP server: 1.pool.ntp.org

3 When prompted, click **OK** and turn off the Hub power



Information

Hub shutdown is complete!
You can turn off its power now.

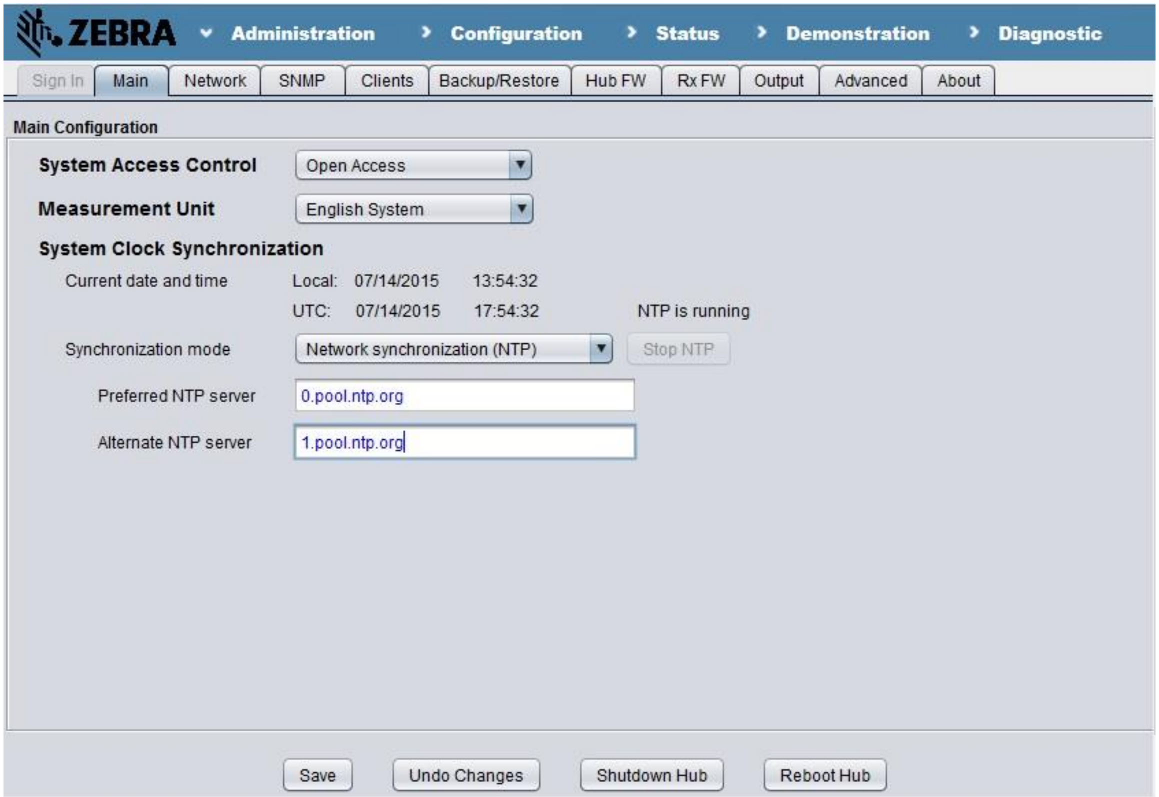
Rebooting the Hub processor

If rebooting the hub processor is needed, follow the steps below.

To reboot the Hub processing software:

1 Start **Hub Administration and Management** application, click **Administration**.

2 In the **Administration** view, on the **Main** tab, click **Reboot Hub**.



Main Configuration

System Access Control: Open Access

Measurement Unit: English System

System Clock Synchronization

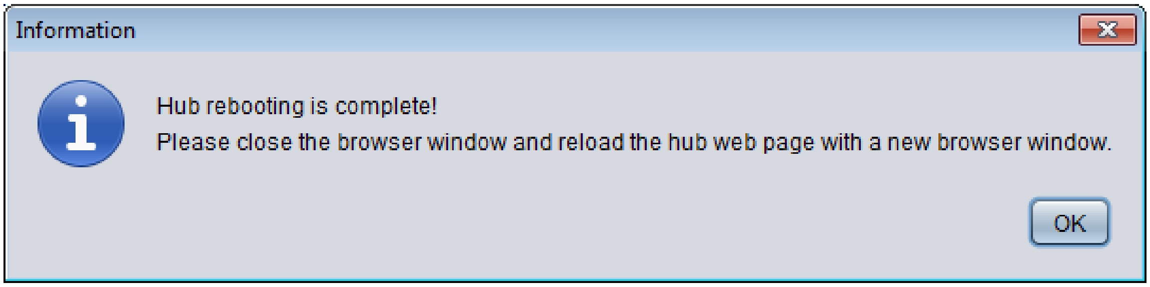
Current date and time
Local: 07/14/2015 13:54:32
UTC: 07/14/2015 17:54:32 NTP is running

Synchronization mode: Network synchronization (NTP)

Preferred NTP server: 0.pool.ntp.org

Alternate NTP server: 1.pool.ntp.org

3 When prompted, click **OK**, then **Hub Administration and Management** application exits. Restart it



Information

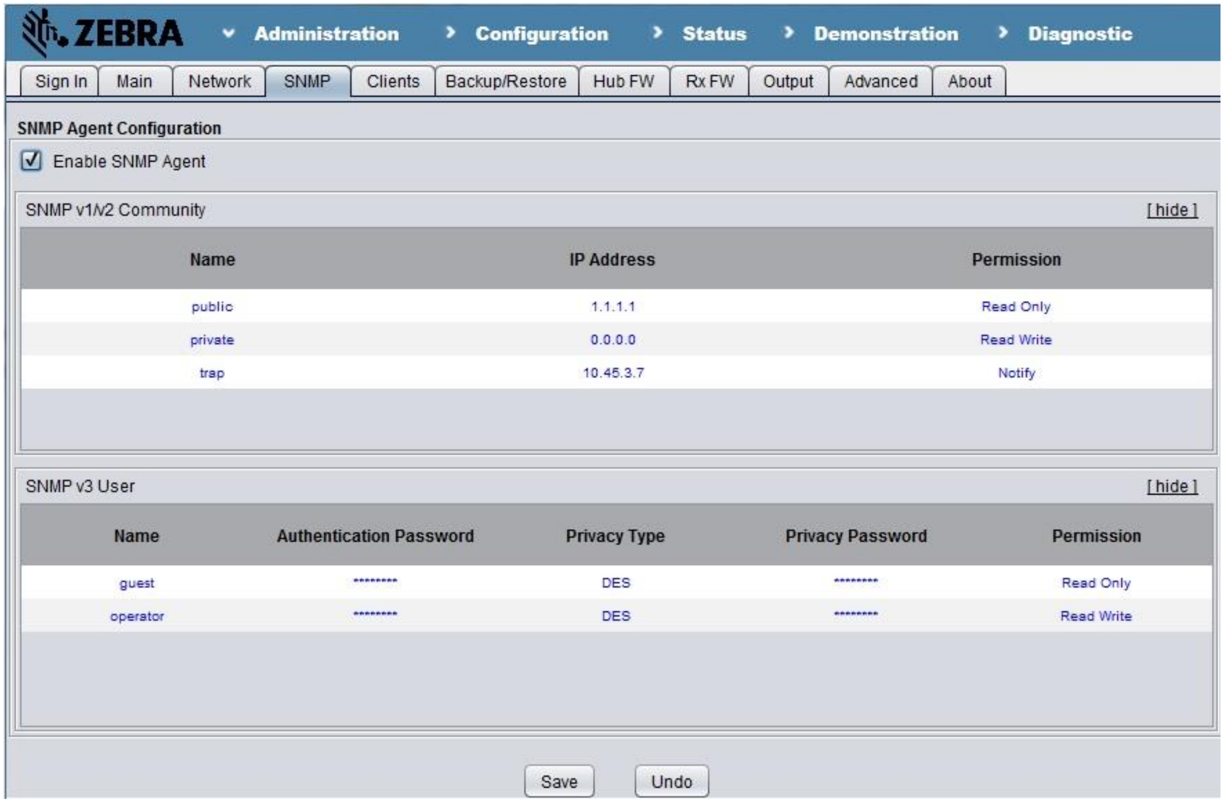
Hub rebooting is complete!
Please close the browser window and reload the hub web page with a new browser window.

Configuring SNMP

The Dart SNMP agent is compliant with the protocols SNMPv1, SNMPv2c, and SNMPv3. It supports MIB II (RFC 1213 MIB) and SNMPv2 MIB and is compliant with generic traps outlined in RFC-1215.

To enable or disable SNMP functionality:

1. Start **Hub Administration and Management** application, click **Administration**.
2. In the **Administration** view, on the **SNMP** tab, select or clear the **Enable the SNMP Agent** check box.
3. Click **Save**.



SNMP Agent Configuration

☑ Enable SNMP Agent

SNMP v1/v2 Community

Name	IP Address	Permission
public	1.1.1.1	Read Only
private	0.0.0.0	Read Write
trap	10.45.3.7	Notify

SNMP v3 User

Name	Authentication Password	Privacy Type	Privacy Password	Permission
guest	********	DES	********	Read Only
operator	********	DES	********	Read Write

To configure SNMP v1 or v2 community:

1. Start **Hub Administration and Management** application, click **Administration**.
2. In the **Administration** view, on the **SNMP** tab, in the **SNMP v1/v2 Community** table, right-click a row and select **Add** to add a community (optional).

To delete a community, right-click the respective row and select Remove.

3. To modify a setting for a community, double-click the table cell in the community row; to complete the edit, press Enter or click any other table cell. You can configure the following settings:
   - **Name:** The name of the community
   - **IP Address:** The IP address of the host from which the community is allowed to access

the hub via SNMP. The value 0.0.0.0 represents any host.

- **Permission:** The permission type granted to the specified community, which can be any of the following:

  None—Does not allow any operations.

  Read only—Allows specified community to get information from the Hub.

  Read Write—Allows getting information from and setting information on the Hub.

  Notify—Allows SNMP trap notifications to be sent to the community on the host specified via IP Address.

4 Repeat Steps 2 and 3 for all communities.

5 Click Save for the community settings to take effect.

Configuring SNMPv3 users

All SNMPv3 users must be authenticated before they access the SNMP MIB. SNMPv3 only supports the authentication algorithm MD5 (Message Digest 5 authentication).

To configure SNMP v3 users:

1 Start **Hub Administration and Management** application, click **Administration**.

2 In the **Administration** view, on the **SNMP** tab, in the **SNMP v3 User** table, right-click a row and select **Add** to add a user (optional).

To delete a user, right-click the respective row and select Remove**.**

3 To modify a setting for a user, double-click the respective cell in the user row; to complete the edit, press Enter or click any other table cell.

- **Name:** The user name
- **Authentication Password:** The password for user authentication
- **Privacy Type:** The protocol type to be used for SNMP communication protection, which can be any of the following:

  None—No protection

  DES—Data Encryption Standard

- **Privacy Password:** The password for deriving encryption keys
- **Permission:** The operation permissions granted to the user:

  None—Does not allow any operations.

  Read Only—Allows operations to get information from the Dart II Hub.

  Read Write—Allow getting information from and set information to the Dart II Hub.

4 Repeat Steps 2 and 3 for all users

5 Click **Save** for the user settings to take effect.

Backing up and restoring Hub configuration data

Dart RTLS lets you back up or restore Hub configuration settings. It preserves all configuration settings, including Receiver and reference tag locations, virtual group settings, and user maps. This feature is useful for preserving data, moving configuration settings from one Hub to another, moving configuration settings to/from System Builder, and backing up settings on the Hub while evaluating alternative settings.

To back up or restore Hub configuration data:

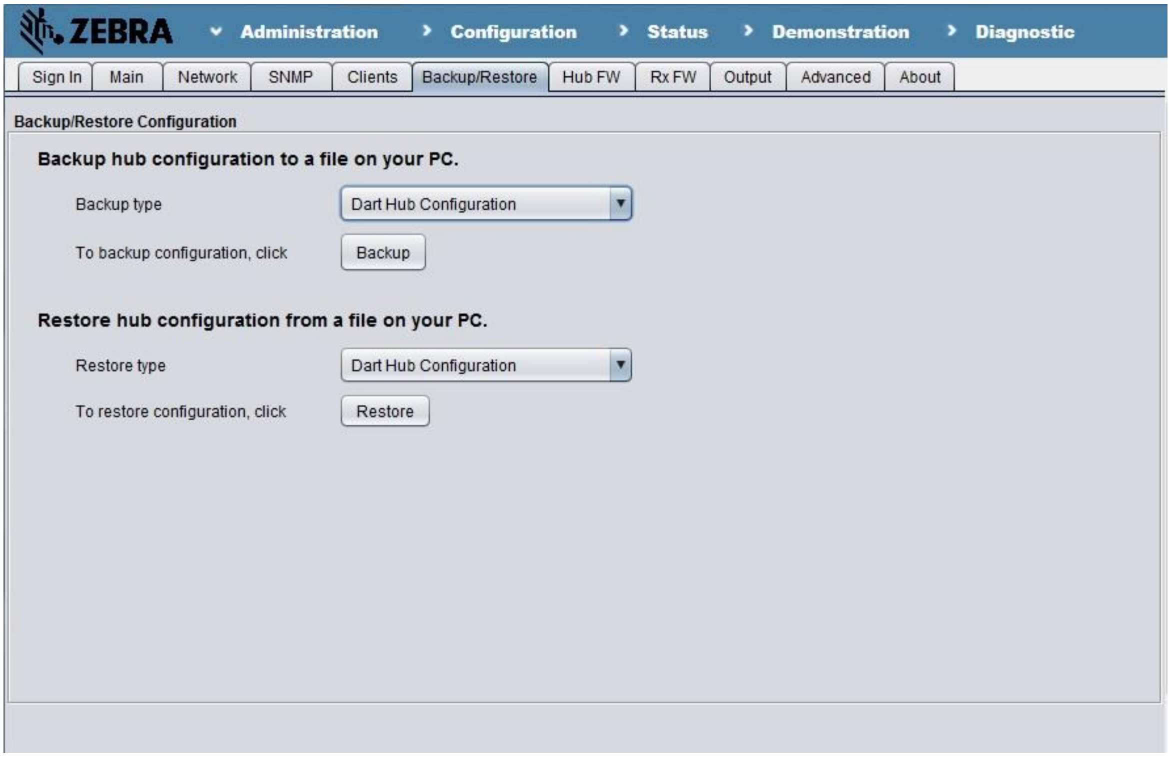
1 Start **Hub Administration and Management** application, click **Administration**.

2 In the **Administration** view, on the **Backup/Restore** tab, do one of the following:

- Backup the hub configuration: Under **Backup hub configuration to a file on your PC**, from the Backup type list, select **Dart Hub Configuration** or **System Builder Configuration**; then click **Backup**.

  You can back up the hub configuration in two different formats: Dart hub native format (by selecting **Dart Hub Configuration**) or System Builder format (by selecting **System Builder Configuration**). Dart hub native format is mainly for backing up hub settings for transferring to another hub; System Builder format is used for transferring the hub configuration back to System Builder for maintenance.

- Restore the hub configuration: Under **Restore hub configuration from a file on your PC**, from the **Restore type** list, select **Dart Hub Configuration** or **System Builder Configuration**; then click **Restore**. You can restore configuration settings from a previously saved hub configuration, a configuration of a different hub, or a hub configuration saved from System Builder.



Backup/Restore Configuration

Backup hub configuration to a file on your PC.

Backup type: Dart Hub Configuration

To backup configuration, click

Restore hub configuration from a file on your PC.

Restore type: Dart Hub Configuration

To restore configuration, click

Uploading new Hub RTLS firmware

You can easily change the Hub RTLS firmware to a different version. Before beginning a firmware upload, make sure the client machine can access the hub RTLS firmware through a CD, hard drive, or local network.

Uploading hub RTLS firmware is non-reversible. Therefore, make sure you install the proper firmware to the Hub.

To upload Dart Hub RTLS firmware:

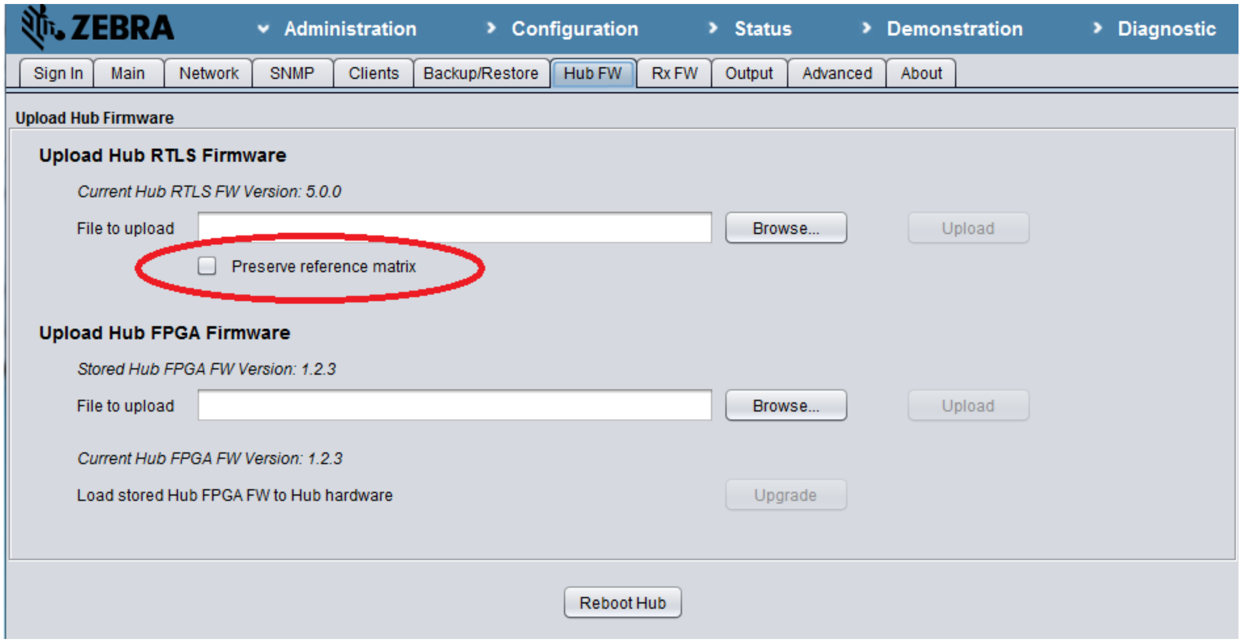
1 Start **Hub Administration and Management** application, click **Administration**.

2 In the **Administration** view, on the **Hub FW** tab, click **Browse…** under **Upload Hub RTLS Firmware** to locate the hub RTLS firmware file to upload.

3 To preserve the established reference matrix (in case of suspended reference) and avoid re-referencing, check the '**Preserver reference matrix**' check box.

4 Click **Upload**. The upload action will subsequently reboot the hub.

5 When prompted, close and re-open the browser window (for FW version 4.1.0 or earlier) or connect to hub using the Zebra Hub Manager (for FW version 5.0.0 and up) to begin using the new firmware.



Upload Hub Firmware

Upload Hub RTLS Firmware

Current Hub RTLS FW Version: 5.0.0

File to upload

□ Preserve reference matrix

Upload Hub FPGA Firmware

Stored Hub FPGA FW Version: 1.2.3

File to upload

Current Hub FPGA FW Version: 1.2.3

Load stored Hub FPGA FW to Hub hardware

Preserve Reference Matrix during FW Upload

UWH1200 Hub V5.0.0 and above, provides ability to preserve the reference matrix during a firmware upload. Previously, after a firmware upload, the hub would reboot and require re-referencing. If the user enabled 'Suspend Reference Tags' and has been able to successfully suspend referencing, then the user may intend to avoid re-referencing due to issues like non-availability of the reference tag during firmware upgrade. In FW 5.0.0 and up, there is an option to enable **Preserve reference matrix** during the Hub FW upload process. Upon hub reboot after new firmware is loaded, the preserved reference matrix is used and Dart hub does not require re-referencing.

Reference matrix can be preserved over Hub firmware updates only when –

- Hub FW version is upgraded
- Hub FPGA version stays the same
- Rx firmware is not upgraded (even if upgrade is available as part of hub FW upgrade)

Uploading new Hub FPGA firmware

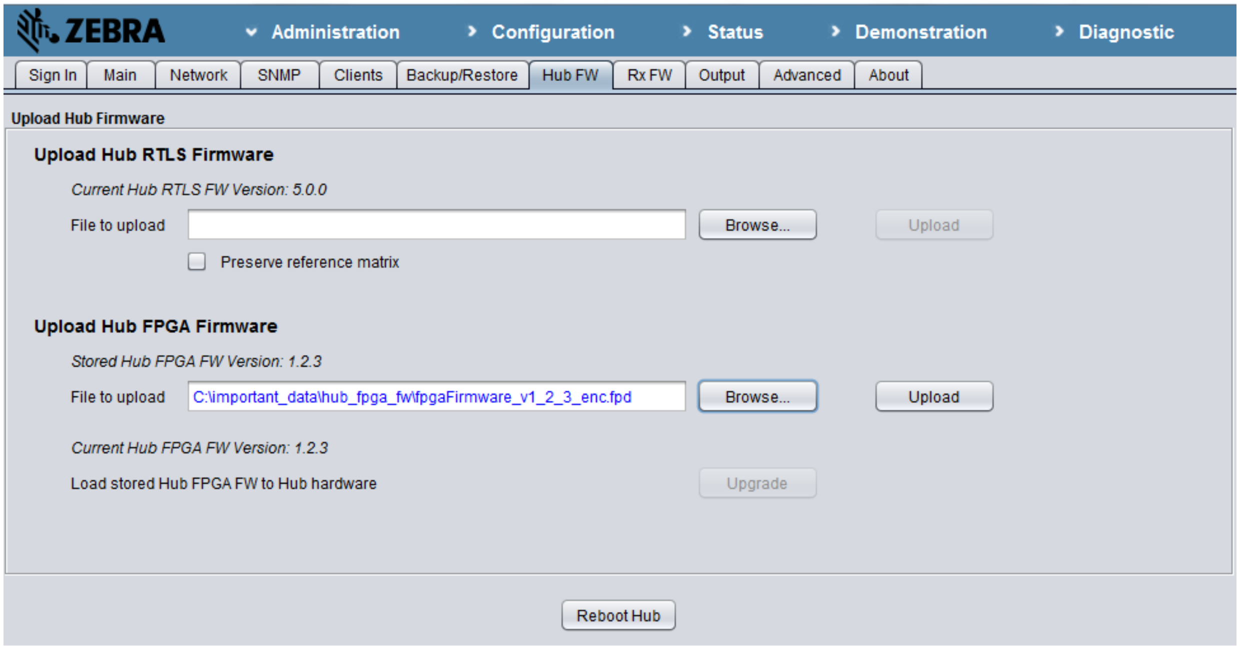
You can easily change the Hub FPGA firmware to a different version. Before beginning a firmware upload, make sure the client machine can access the hub FPGA firmware through a CD, hard drive, or local network.

⚠ Uploading hub FPGA firmware is non-reversible. Therefore, make sure you install the proper firmware to the Hub.

To upload Dart Hub FPGA firmware:

1 Start **Hub Administration and Management** application, click **Administration**.

2 In the **Administration** view, on the **Hub FW** tab, click **Browse…** under **Upload Hub FPGA Firmware** to locate the hub FPGA firmware file to upload.



Upload Hub Firmware

Upload Hub RTLS Firmware

Current Hub RTLS FW Version: 5.0.0

File to upload

□ Preserve reference matrix

Upload Hub FPGA Firmware

Stored Hub FPGA FW Version: 1.2.3

File to upload C:\important_data\hub_fpga_fw\fpgaFirmware_v1_2_3_enc.fpd

Current Hub FPGA FW Version: 1.2.3

Load stored Hub FPGA FW to Hub hardware

3 Click **Upload**. The upload action will subsequently restart the hub firmware. For Hub FW 5.0.0 and up, during the firmware restart, the newly uploaded FPGA firmware will be pushed to hub hardware.

4 If the newly uploaded hub FPGA firmware is different than the firmware currently running on hub FPGA, the **Upgrade** button is activated. Click **Upgrade** to push the newly uploaded

FPGA firmware to hub hardware (Only for Hub FW 4.1.0 and lower).

Uploading new Receiver firmware

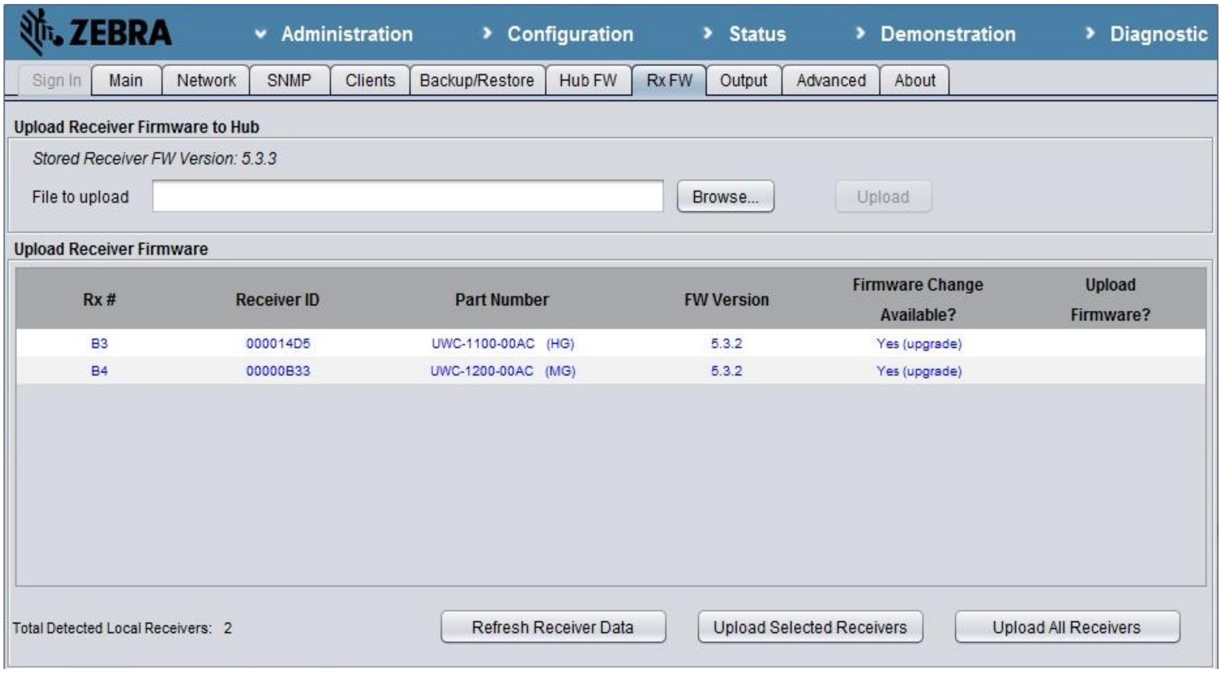
Uploading the receiver firmware to a different version is straight forward process. It includes two steps: upload receiver firmware to the hub, and install the firmware to Receivers. Before you start, make sure the client machine can access the receiver firmware through a CD, hard drive, or local network.

Uploading receiver firmware is non-reversible. Therefore, make sure you install the proper firmware upgrade to the Receivers.

To upload the receiver firmware to the hub:

1 Start **Hub Administration and Management** application, click **Administration**.

2 In the **Administration** view, on the **RX FW** tab, click **Browse…** to locate the receiver firmware file to upload.



Upload Receiver Firmware to Hub

Stored Receiver FW Version: 5.3.3

File to upload

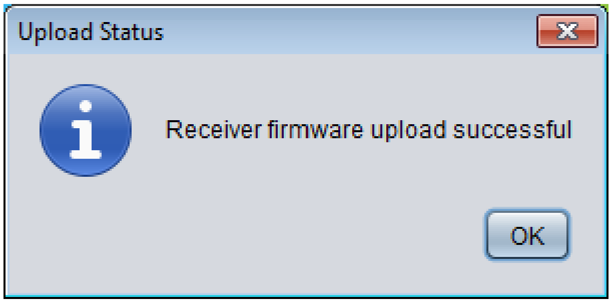
Upload Receiver Firmware

Rx #	Receiver ID	Part Number	FW Version	Firmware Change Available?	Upload Firmware?
B3	000014D5	UWC-1100-00AC (HG)	5.3.2	Yes (upgrade)	
B4	00000B33	UWC-1200-00AC (MG)	5.3.2	Yes (upgrade)	

Total Detected Local Receivers: 2

3 **Click Upload.**

4 Click **OK** when prompted to accept the uploaded receiver firmware.



Receiver firmware upload successful

To upload the new firmware to receiver(s):

After uploading the receiver firmware to the hub, the **Upload Receiver Firmware** table contains firmware change status for each detected receiver.

The hub checks firmware version of each detected receiver to determine if a firmware change is available, and shows the result in the "Firmware Change Available?" column.

- **Rx #:** Hexadecimal receiver number as configured; if not configured, leave blank.
- **Receiver ID:** The unique 4-byte hexadecimal ID programmed into the receiver.
- **Part Number:** receiver part number with antenna type.
- **FW Version:** Version of firmware currently running on the receiver.
- **Firmware Change Available? :** Indicates if the receiver has a different firmware version from the one used by the hub, and a firmware change is available.

  N/A —Firmware change is not supported by the receiver

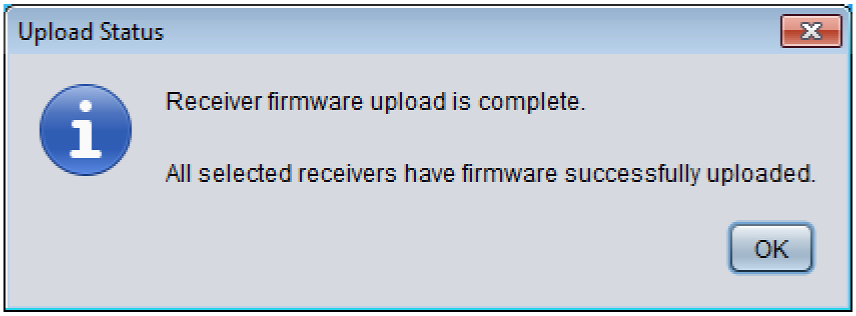
  Yes (downgrade) — A firmware change is available for this receiver. After a firmware upload, the receiver firmware will be downgraded to a previous firmware version.

  Yes (upgrade) — A firmware change is available for this receiver. After a firmware upload, the receiver firmware is upgraded to a newer version.

  No—Receiver has the same firmware as the receiver firmware stored in the hub.
- **Upload Firmware? :** User's checklist of receiver(s) to upload firmware.

5 Click **Upload Selected Receivers** or **Upload All Receivers** to upload the firmware to the selected or all change available receiver(s).

6 Click **OK** when prompted. Once firmware upload is complete, the table will be updated.



Receiver firmware upload is complete.

All selected receivers have firmware successfully uploaded.

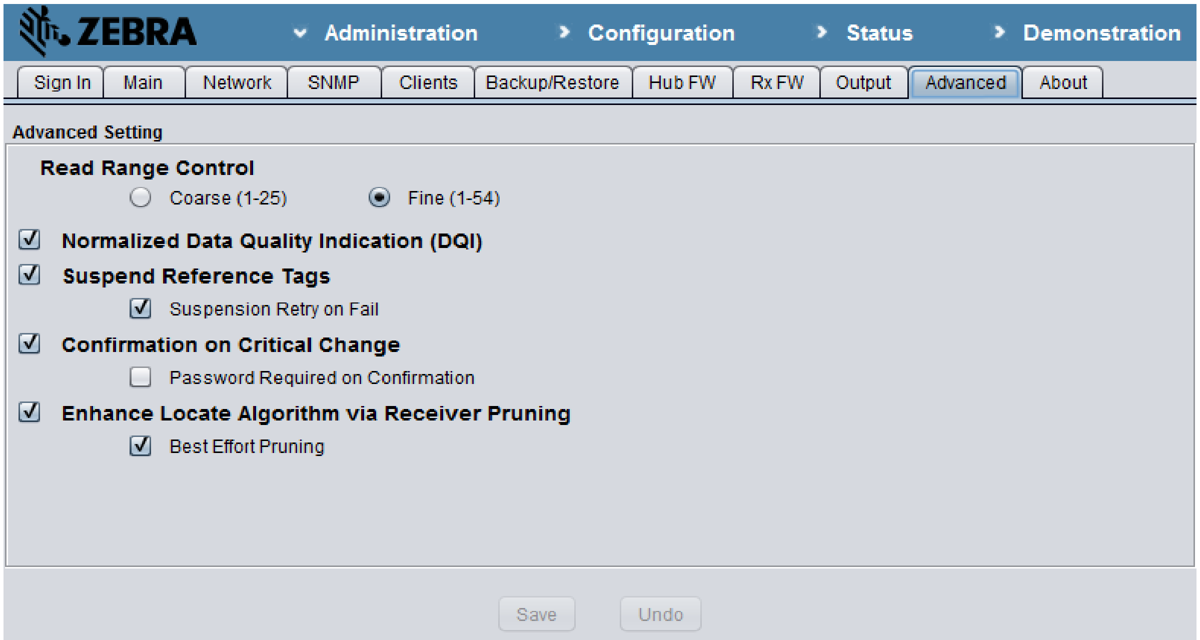
Receiver range control

The Dart hub provides two control modes for receiver read range: coarse mode and fine mode. Coarse control mode is the default mode, which allows receiver read ranges from 1 to 25, where 1 is the lowest read range setting and 25 is the largest read range setting. In fine control mode, receiver read range setting range is 1 to 54, where 1 is the lowest and 54 is the greatest.

To change receiver range control mode:

1 Start **Hub Administration and Management** application, click **Administration.**

2 In the **Administration** view, click the **Advanced** tab to open the web page.



Advanced Setting

Read Range Control

○ Coarse (1-25) ● Fine (1-54)

☑ Normalized Data Quality Indication (DQI)

☑ Suspend Reference Tags

☑ Suspension Retry on Fail

☑ Confirmation on Critical Change

□ Password Required on Confirmation

☑ Enhance Locate Algorithm via Receiver Pruning

☑ Best Effort Pruning

3 Select desired read range control mode, coarse or fine.

4 Check **Normalized Data Quality Indication (DQI)** to select normalized DQI mode or deselect the option for default DQI mode.

5 Click **Save** for the user settings to take effect.

Reference tag suspension

Reference tag ties timing of receivers, which is critical for correct tag location. To achieve correct and reliable referencing, line of sight of reference tag for each associated receiver needs to be maintained. At some applications, because of limitation of system installation, object or personnel movement will break this line of sight from time to time, and degrade the Dart RTLS system performance. To avoid this impact, you can turn on reference tag suspension option. When this option is on, the RTLS system will check to see if consistent and complete referencing is obtained in a short period (30 seconds) after each hub firmware restart. If the referencing is obtained, this referencing is fixed and will be used in the following tag location calculation. Till next hub firmware restart, the hub will not modify referencing based on receiving time of each reference tag transmission.

When reference suspension is enabled but fails, the hub will not calculate tag location. Instead, for each tag blink, the hub will send presence data (Non-locate P data), if one or more RTLS receivers have “Presence Detection” configured (see page 33 for configuring Presence Detect for a Receiver).

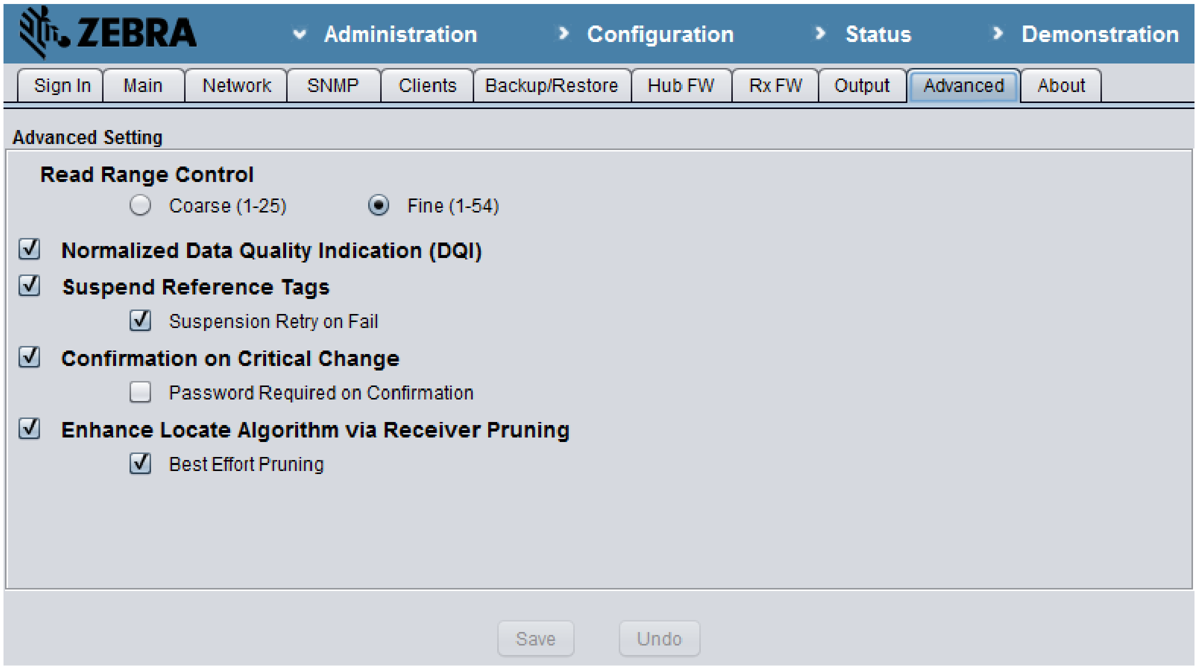
Reference Suspension Automatic Retry on Failure:

The initial reference suspension after system reboot or firmware restart could fail for different reasons. To be able to automatically retry after initial failure is a big convenience for the customer. Dart RTLS system provides user the choice to enable automatic retry.

Reference suspension should only be used when on-site maintenance is an integral part of using the RTLS system.

To turn on/off reference tag suspension:

1. Start **Hub Administration and Management** application, click **Administration**.
2. In the **Administration** view, click the **Advanced** tab to open the web page.



Advanced Setting

Read Range Control

○ Coarse (1-25) ● Fine (1-54)

☑ Normalized Data Quality Indication (DQI)

☑ Suspend Reference Tags

☑ Suspension Retry on Fail

☑ Confirmation on Critical Change

□ Password Required on Confirmation

☑ Enhance Locate Algorithm via Receiver Pruning

☑ Best Effort Pruning

3. Check **Suspend Reference Tags** to turn on reference tag suspension or uncheck it to turn it off.
4. If **Suspend Reference Tags** is enabled, then check or uncheck **Suspension Retry on Fail** box to enable or disable automatic retry.
5. Click **Save** for the user settings to take effect.

Reference Suspension Protection

Some configuration changes to the Dart RTLS hub require system restart and re-referencing. In cases where the system is configured for Reference Tag Suspension, there may be undesirable consequences on making configuration changes.

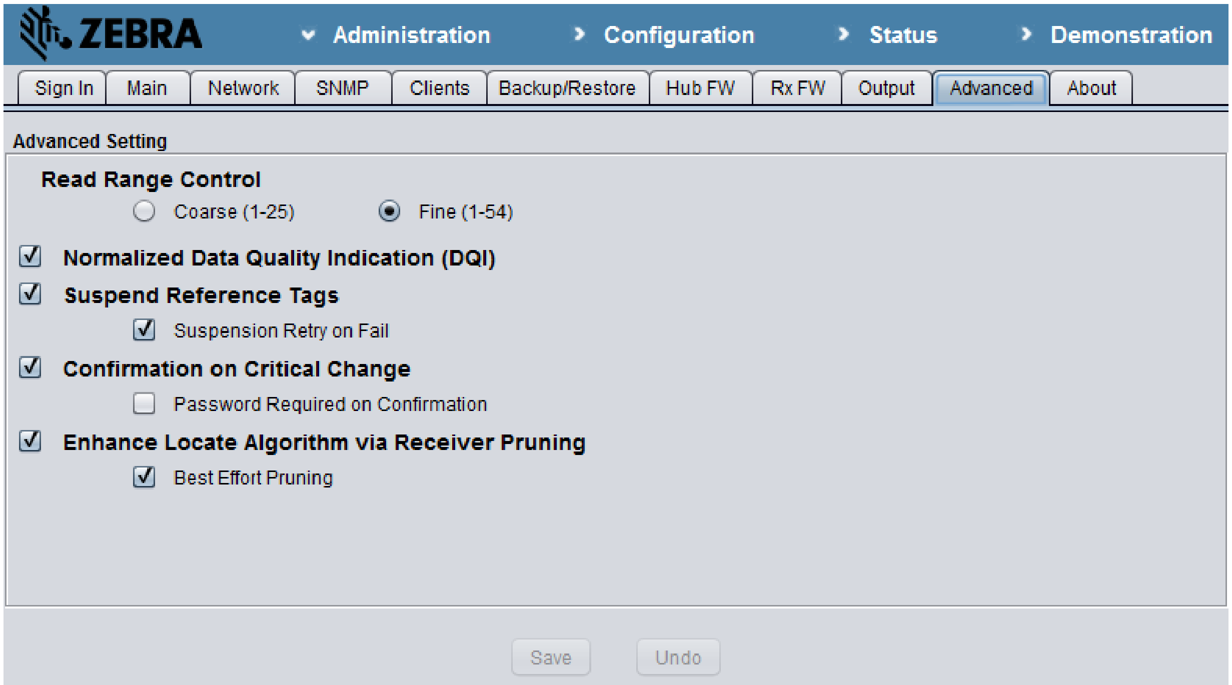
To alert the user of changes that affect reference suspension, the setting “Confirmation on critical change” has been added. When selected, the user will be warned of changes that will affect the suspended reference tag status.

Password Checking on Confirmation

If System Access Control is set to ‘Sign-in Based Access’, then for added security, besides explicit change confirmation, password based check can be enabled to check if the person has the privilege to make the critical change. The confirmation password is the same as the access control password used for logging in (as administrator or operator).

To configure the system to enable reference suspension protection:

1. Start **Hub Administration and Management** application, click **Administration**.
2. In the **Administration** view, select the **Advanced** tab



Advanced Setting

Read Range Control

○ Coarse (1-25) ● Fine (1-54)

☑ Normalized Data Quality Indication (DQI)

☑ Suspend Reference Tags

☑ Suspension Retry on Fail

☑ Confirmation on Critical Change

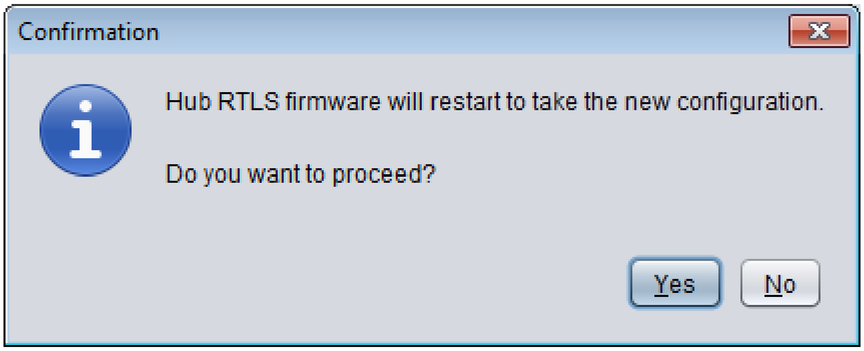
□ Password Required on Confirmation

☑ Enhance Locate Algorithm via Receiver Pruning

☑ Best Effort Pruning

3. Check or uncheck **Confirmation on Critical Change** box to enable or disable reference suspension protection.
4. If System Access control is set to '**Sign-In Based Access**' then configuration change can be password protected. Check or un-check **Password Required on Confirmation** to enable or disable password confirmation on critical change. Changing on **Password Required on Confirmation** selection also requires password confirmation. Enter the password when prompted. Password entered should be the same as the one used for current user log-in.
5. Click **Save** for the user settings to take effect.

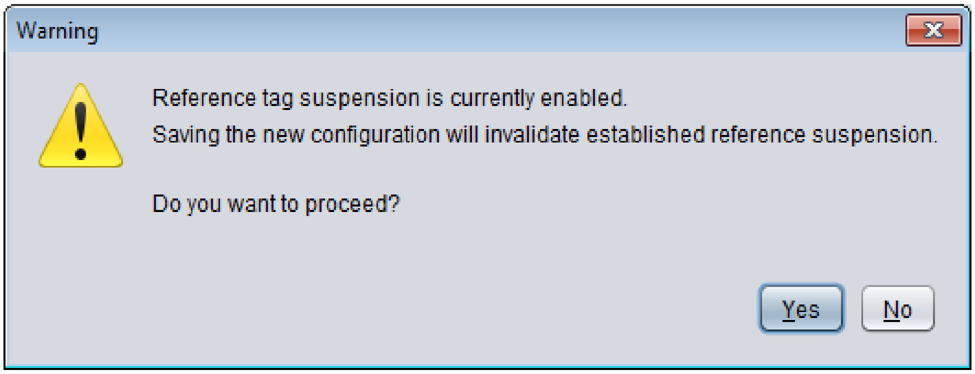
After **Confirmation on Critical Changes** is selected, accepting any changes that cause firmware restart will require user explicit confirmation. If **Suspend Reference Tag** is not enabled at the time, then a confirmation message box is shown which looks as follows:


Confirmation

Hub RTLS firmware will restart to take the new configuration.

Do you want to proceed?

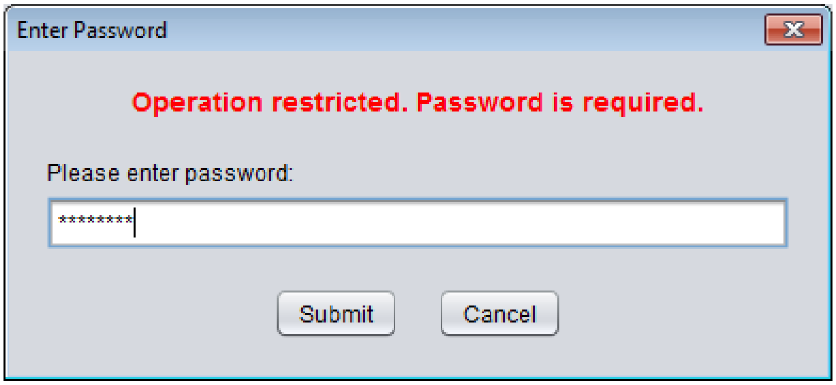
If **Suspend Reference Tag** is enabled, then a confirmation message box is shown which looks as follows


Warning

Reference tag suspension is currently enabled.
Saving the new configuration will invalidate established reference suspension.

Do you want to proceed?

If **Password Required on Confirmation** is selected, after confirming changing by clicking **YES** button on either of above confirmation message box, a password input message box will show up. Failing to provide correct password will cause the saving operation to abort.


Enter Password

Operation restricted. Password is required.

Please enter password:

****

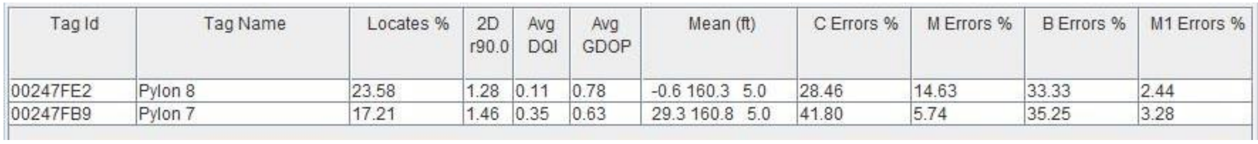
Receiver Pruning Based Location Algorithm

Accuracy of tag location calculated at Dart RTLS system relies on direct line of sight of tags from each receiver. In reality, blockage and reflection happens in the deployment environment, and receivers may pick reflected signal instead of direct signal. These wrongly picked signals will most likely dramatically degrade the calculated location. To mitigate this kind of issue, UWH-1200 hub introduces a new algorithm to analyze the tag blink timing from receivers, and drop those wrong timings.

New algorithm incorporates **pre-pruning** and **pruning**. **Pre-pruning** is an improvement in location algorithm which detects and removes late receivers. Only significant reflection issues can be resolved with **pre-pruning**. Algorithm always performs pre-pruning.

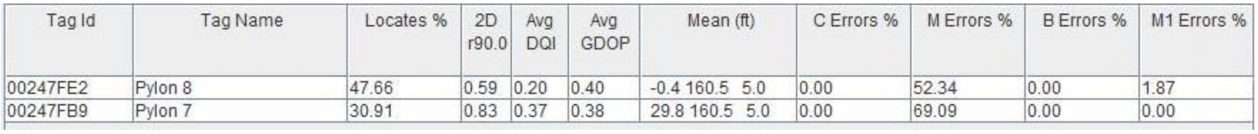
Example:

Without **pre-pruning**: 'Locates %' are less due to non-convergence.



Tag Id	Tag Name	Locates %	2D r90.0	Avg DQI	Avg GDOP	Mean (ft)	C Errors %	M Errors %	B Errors %	M1 Errors %
00247FE2	Pylon 8	23.58	1.28	0.11	0.78	-0.6 160.3 5.0	28.46	14.63	33.33	2.44
00247FB9	Pylon 7	17.21	1.46	0.35	0.63	29.3 160.8 5.0	41.80	5.74	35.25	3.28

With **pre-pruning**: 'Locates %' improve, as bad receivers are removed. But min receiver errors increase as there might not be enough receivers left to locate after the late ones are removed.

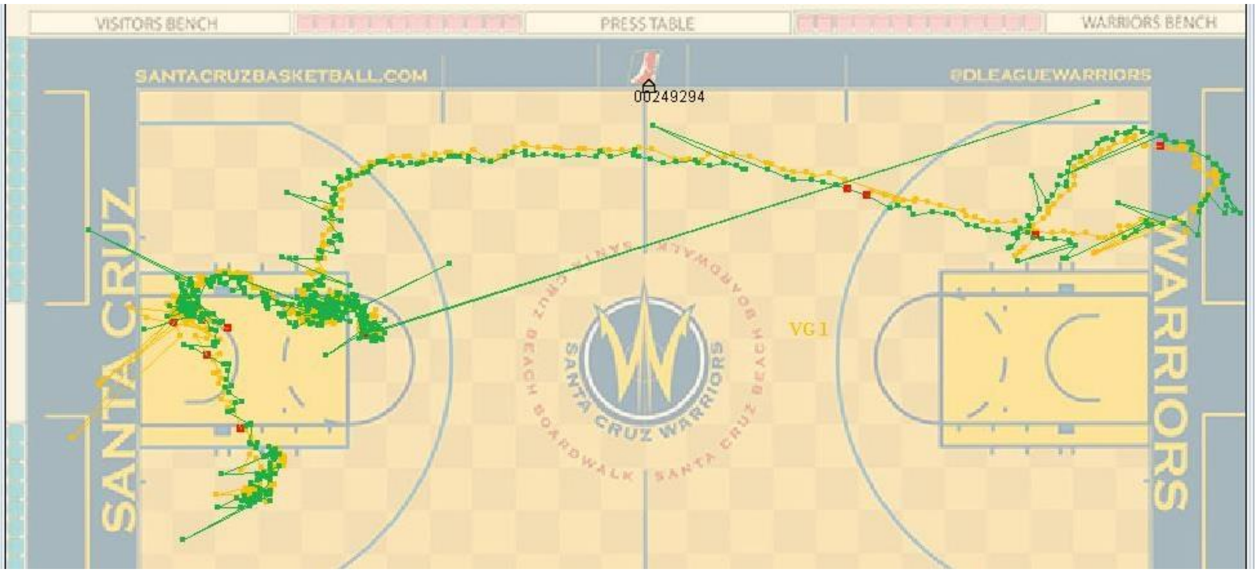


Tag Id	Tag Name	Locates %	2D r90.0	Avg DQI	Avg GDOP	Mean (ft)	C Errors %	M Errors %	B Errors %	M1 Errors %
00247FE2	Pylon 8	47.66	0.59	0.20	0.40	-0.4 160.5 5.0	0.00	52.34	0.00	1.87
00247FB9	Pylon 7	30.91	0.83	0.37	0.38	29.8 160.5 5.0	0.00	69.09	0.00	0.00

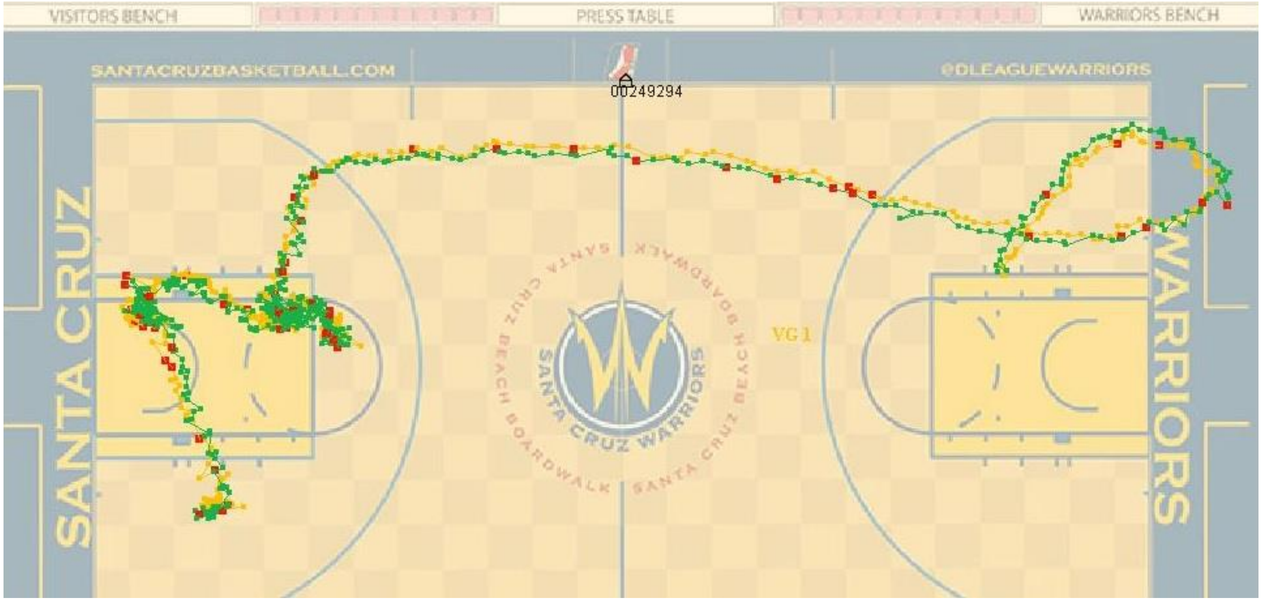
Pruning relies on over determination and can further improve location calculation. Tag blink timings from receivers are analyzed and incorrect ones are dropped, provided more than enough receivers provide blink timing. With **Pruning** enabled, the system performs the Calculate - Validate - Optimize iteration until a valid location is obtained or pruning limit is reached.

Example:

Without **Pruning**:



With **Pruning**:



By default, this receiver pruning based location algorithm is disabled. The user can enable it using **Hub Administration and Management** application. After the pruning algorithm enabled, whenever Dart RTLS system fails to produce a good tag location from a tag blink in the standard fashion, it starts analyzing and pruning received timings and will most likely output a valid tag location.

<u>Pruning Criteria</u>: The following criteria are used to judge whether the location computation is good or bad.

1. Bounding Box – If locate computed is outside the bounding box of the virtual group, then it's a bad locate. This criterion is used as the default.
2. DQI (Data Quality Indicator) – If DQI filter is enabled, then the DQI threshold is used to determine if a locate is good or bad. In theory, DQI value of 2.0 or under indicates good accuracy in position measurement.
3. GDOP (Geometric dilution of precision) – If GDOP filter is enabled, then the GDOP threshold is used to determine if a locate is good or bad. In theory, GDOP threshold between 1.0 and 2.0 is a good setting for well-designed deployment.

<u>Algorithm pruning limit</u>: Dart RTLS system enforces a limit on how many received timing can be pruned. Limit varies on size of detecting receiver set and virtual group configuration. If minimum number of unit in a virtual group(VG) is – M, number of receivers receiving the tag blink in this VG is - N, stop pruning if valid location is obtained or when K receivers left , where K = MAX(M, N* 3/4).

K is calculated as an integer, floating value will be truncated.

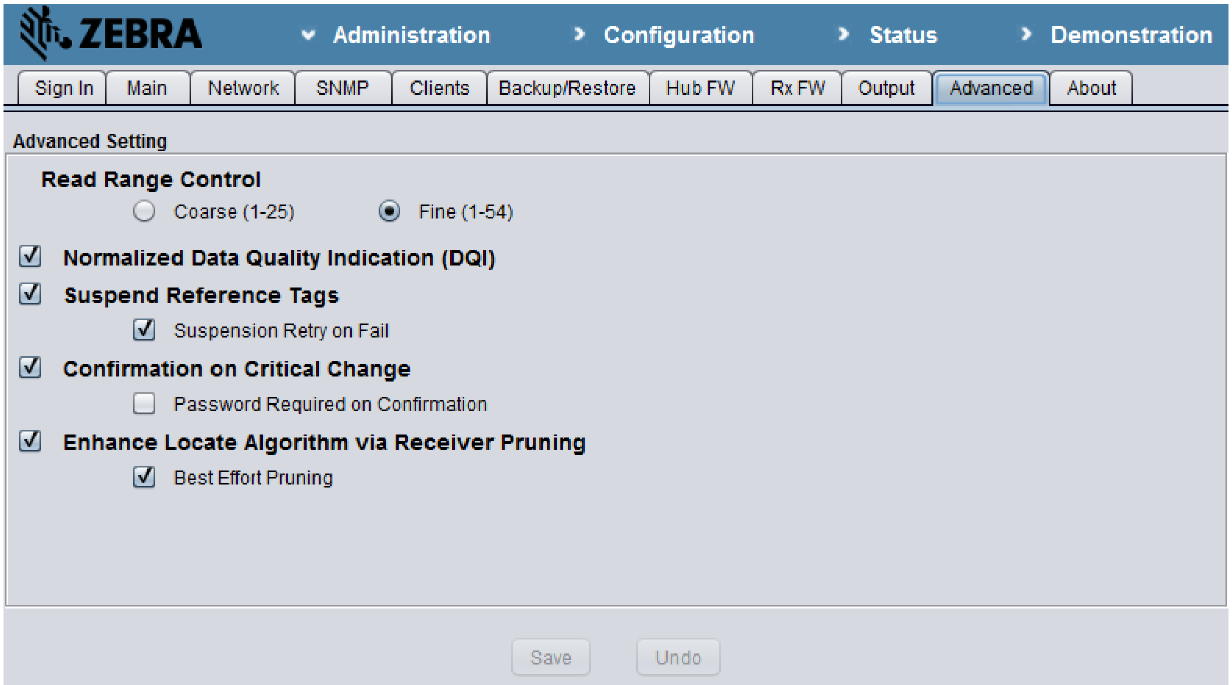
Example: For a VG with 9 receivers detecting a tag blink, if min units is set to 3,

M = 3, N= 9, so K = MAX(3, 9*3/4) = MAX(3, 6.75) = MAX(3, 6) = 6 . So pruning may continue until 6 receivers are left.

To configure the system to enable receiver pruning based location algorithm:

1 Start **Hub Administration and Management** application, click **Administration**.

2 In the **Administration** view, select the **Advanced** tab



Advanced Setting

Read Range Control

○ Coarse (1-25) ● Fine (1-54)

☑ Normalized Data Quality Indication (DQI)

☑ Suspend Reference Tags

☑ Suspension Retry on Fail

☑ Confirmation on Critical Change

□ Password Required on Confirmation

☑ Enhance Locate Algorithm via Receiver Pruning

☑ Best Effort Pruning

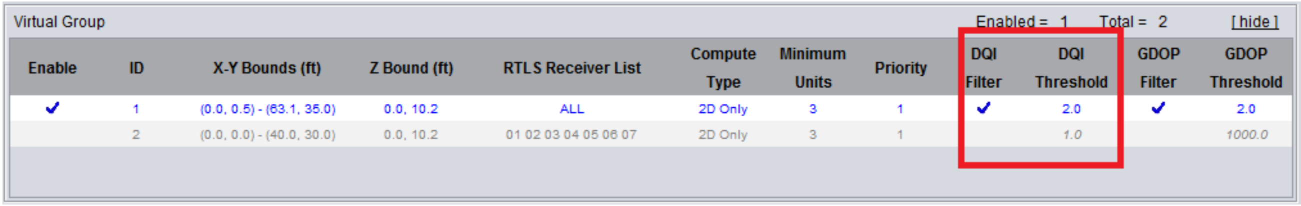
3 Check or un-check **Enhance Locate Algorithm via Receiver Pruning** to enable or disable the receiver pruning based location algorithm.

4 Click **Save** for the user settings to take effect.

Best Effort Pruning

Best effort pruning is an effort to balance locate accuracy and volume. It can be enabled/disabled only when receiver pruning based locate enhancement algorithm is enabled. Best effort pruning, when enabled, changes the behavior of DQI filtering, if selected, in virtual group configuration. In this case, instead of filtering calculated tag locates, the DQI filter serves as the best effort goal for the pruning algorithm. If an initially calculated tag locate fails to meet the virtual group requirements, such as outside of virtual group boundary or with DQI higher than the DQI threshold, the pruning algorithm starts to optimize the tag locate by removing outlier receivers one by one. If the final tag locate produced by pruning algorithm has DQI higher than the DQI threshold, the Hub will send the tag locate in the output data stream, as oppose to dropping the tag locate and outputting a presence data in the output data stream.

Best effort pruning only affects tag locate calculation inside a virtual group with DQI filtering enabled.



Virtual Group

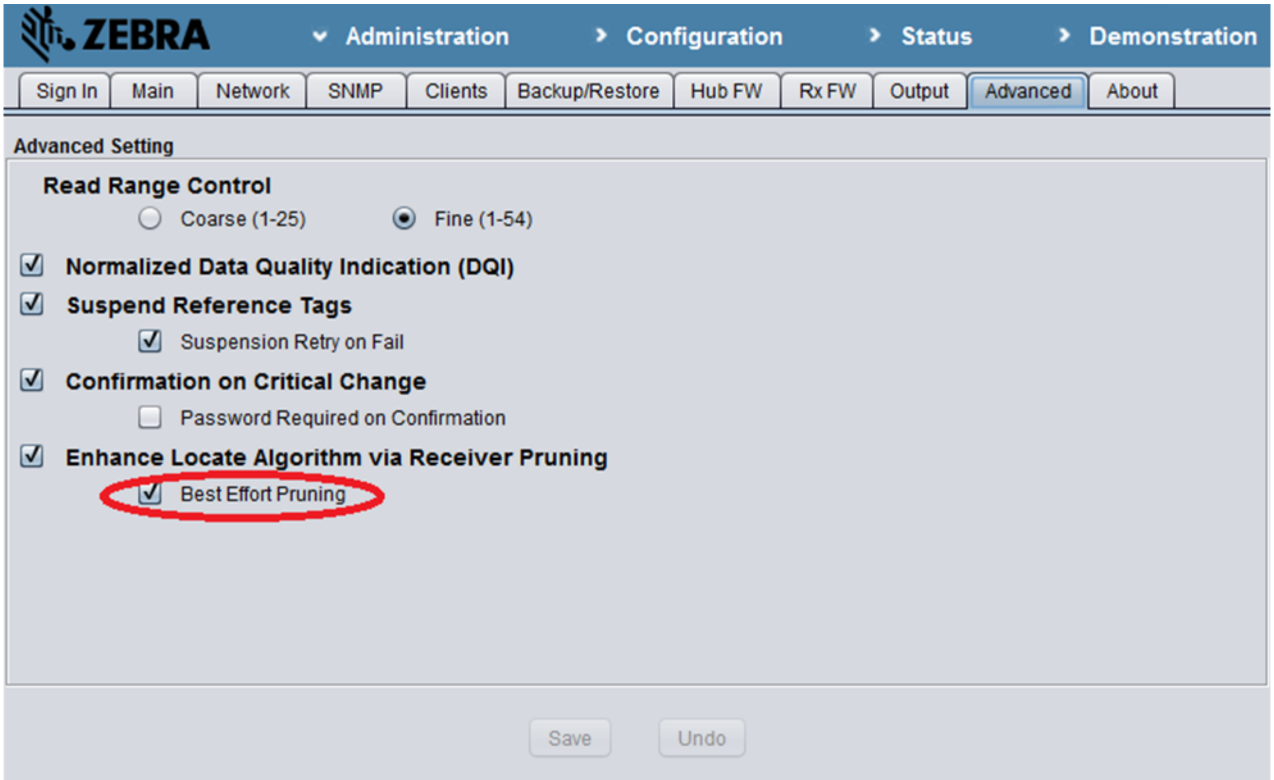
Enabled = 1 Total = 2 [hide]

Enable	ID	X-Y Bounds (ft)	Z Bound (ft)	RTLS Receiver List	Compute Type	Minimum Units	Priority	DQI Filter	DQI Threshold	GDOP Filter	GDOP Threshold
✓	1	(0.0, 0.5) - (63.1, 35.0)	0.0, 10.2	ALL	2D Only	3	1	✓	2.0	✓	2.0
	2	(0.0, 0.0) - (40.0, 30.0)	0.0, 10.2	01 02 03 04 05 06 07	2D Only	3	1		1.0		1000.0

To enable best effort pruning

1 Start **Hub Administration and Management** application, click **Administration**.

2 In the **Administration** view, select the **Advanced** tab



Advanced Setting

Read Range Control

○ Coarse (1-25) ● Fine (1-54)

☑ Normalized Data Quality Indication (DQI)

☑ Suspend Reference Tags

☑ Suspension Retry on Fail

☑ Confirmation on Critical Change

□ Password Required on Confirmation

☑ Enhance Locate Algorithm via Receiver Pruning

☑ Best Effort Pruning

3 Click **Enhance Locate Algorithm via Receiver Pruning** first if it is not enabled.

4 Click **Best Effort Pruning.**

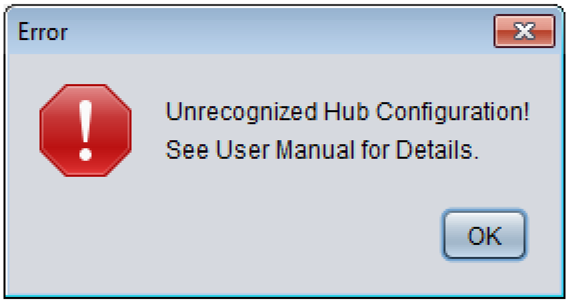
5 Click **Save** to make the change take effect.

Configuration Recovery

Configuration Recovery provides a method to recover from undesirable configuration changes.

Configuration Recovery is non-reversible.

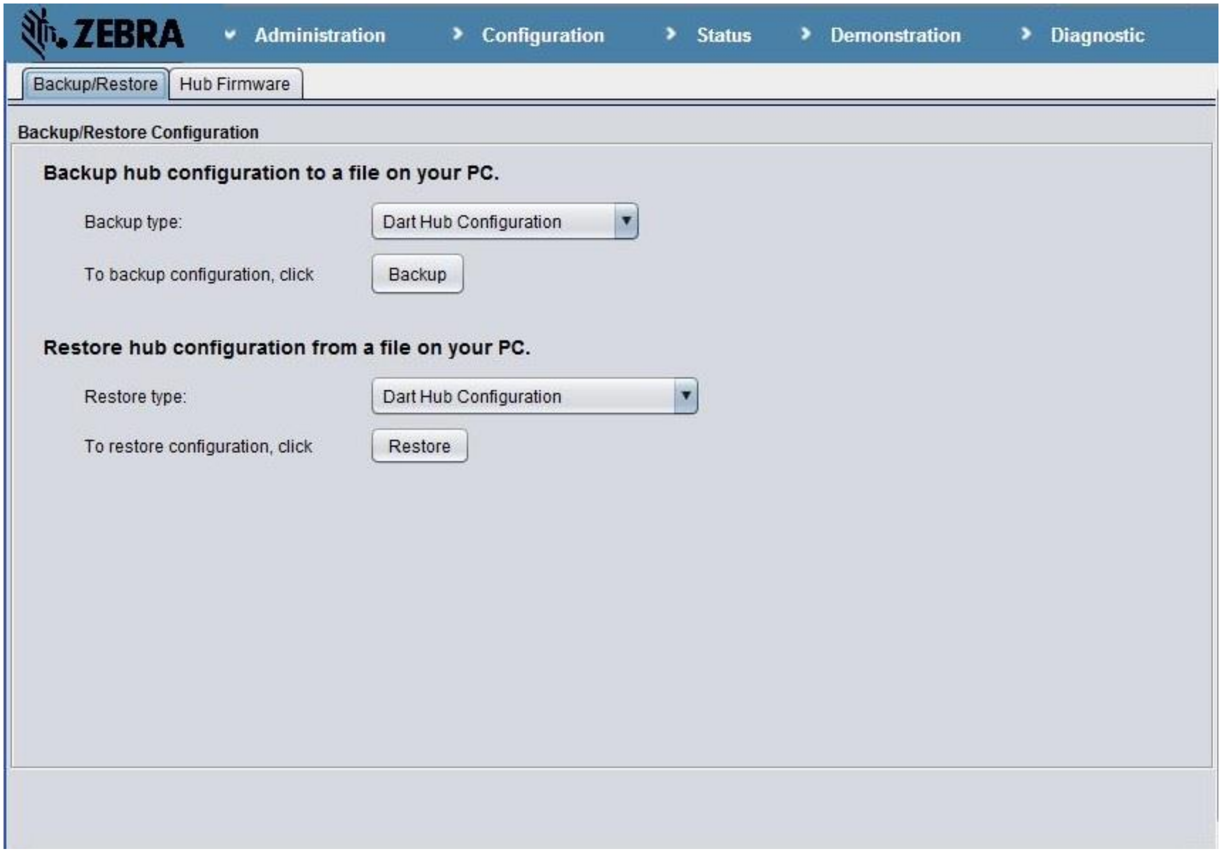
In the unlikely situation that an unexpected configuration is imported into the hub, the hub will display the following error message:



Error

Unrecognized Hub Configuration!
See User Manual for Details.

By clicking Ok, the **Configuration Recovery** feature is available. The **Configuration Recovery** allows the user to restore a new configuration or the factory default Dart hub configuration. It also allows the user to backup current Dart hub configuration for further investigation.



Backup/Restore Configuration

Backup hub configuration to a file on your PC.

Backup type: Dart Hub Configuration

To backup configuration, click

Restore hub configuration from a file on your PC.

Restore type: Dart Hub Configuration

To restore configuration, click

Admin User Access

An admin account is provided with Dart hub that is accessible through the RS232 port. This user account has limited capability and is provided to allow IP address reset, user password resets, and to restore factory configuration settings.

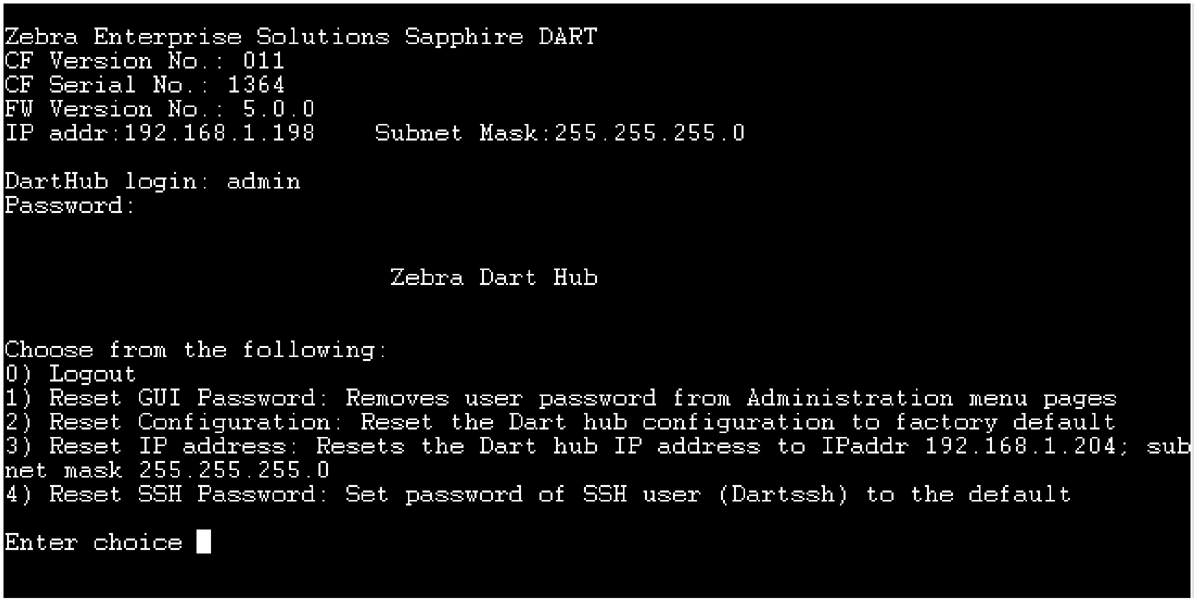
The UWH-1200 RS-232 port is a host male connector, to connect to a computer, a female to female null cable is required (such as L-com CSNULL9FF-5A WWW.L-COM.COM).

Console port setup

Dart hub console port is located on the back of the hub and is fully compatible with RS-232 standard. Its setup is as following:

Baud Rate	115200
Date Bits	8
Parity	None
Stop Bits	1
Flow Control	None

To access the user account, login to the Dart hub RS232 console using user "**admin**" and password "**zebra**".



```
Zebra Enterprise Solutions Sapphire DART
CF Version No.: 011
CF Serial No.: 1364
FW Version No.: 5.0.0
IP addr:192.168.1.198    Subnet Mask:255.255.255.0

DartHub login: admin
Password:


                          Zebra Dart Hub


Choose from the following:
0) Logout
1) Reset GUI Password: Removes user password from Administration menu pages
2) Reset Configuration: Reset the Dart hub configuration to factory default
3) Reset IP address: Resets the Dart hub IP address to IPaddr 192.168.1.204; sub
net mask 255.255.255.0
4) Reset SSH Password: Set password of SSH user (Dartssh) to the default

Enter choice █
```

admin user choices are as follows:

Reset GUI Password: removes all accounts except the default administrator account and resets its password to factory default. Reverts the System Access Control setting to “Open Access”.

Reset Configuration: resets hub configuration settings (with the exception of IP address) to the factory default configuration.

Reset IP address: resets the Dart hub network setting (IP address, subnet mask) to the default

IP Address: 192.168.1.204

Subnet mask: 255.255.255.0

Gateway: 192.168.1.1

Reset SSH Password: resets the password of SSH user (for secured data output) to the default

SSH user name: Dartssh

SSH user password: Dartsshpwd1

10 Demo software

Dart RTLS uses a JAVA™ client applet as a utility for displaying initial system check-out and results (the location of tags and receivers). This utility serves as a demo. Most likely, you will need to obtain client software that is tailored to a more specific application.

You can control the display of this demo utility by:

- *Editing real-time demo graphics* (on page 77)
- *Viewing and filtering the raw data stream from the Hub* (on page 79)
- *Changing the display background* (on page 81) by adding customized images

In This Section

Editing the display of real-time demo graphics

You can modify the display of graphics in the real-time demo application.

To edit the display of real-time demo graphics:

1 Start the **Hub Administration and Management** application, click **Demonstration**.

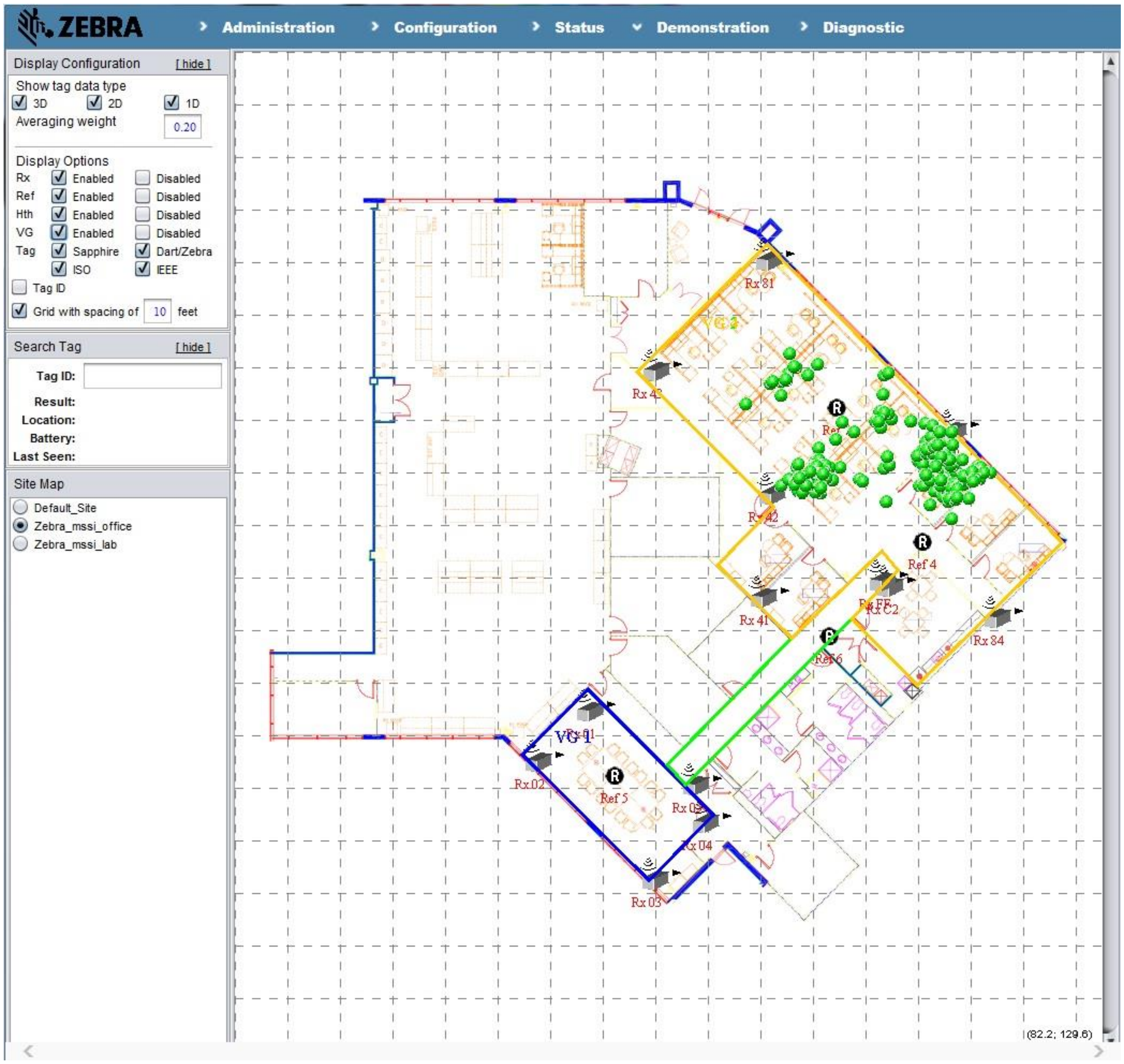
2 In the **Demonstration** view, on the **Display Configuration** tab, specify the following information. To complete the edit, press Enter or click outside of editing area:

- **Show tag data type:** Select the applicable check boxes to display 3D, 2D, and/or 1D data.

"P" data is not available for display in this grid.

- **Averaging weight:** Enter a value to reduce jitter from one read to the next in tag locations; the lower the averaging weight, the higher the averaging. To turn averaging off, set the averaging weight to 1. For smallest amounts of jitter to be visible on the display, an averaging weight of 0.1 to 0.3 is recommended. The range is 0.1 to 1.
- **Display Options:** Select the check boxes to show Enabled/Disabled Receivers, Enabled/Disabled reference tags, Enabled/Disabled virtual groups, ISO/IEEE/Dart/Sapphire Tags, and Tag IDs.

- **Background Grid:** Select the check box to display background grid; then enter a value to modify the spacing.
- **Site Map:** Select the desired site map to be displayed as geographic background by clicking on the corresponding radio button. The **Default_Site** provides blank background.



Display Configuration [hide]

Show tag data type
☑ 3D ☑ 2D ☑ 1D
Averaging weight 0.20

Display Options
Rx ☑ Enabled □ Disabled
Ref ☑ Enabled □ Disabled
Hth ☑ Enabled □ Disabled
VG ☑ Enabled □ Disabled
Tag ☑ Sapphire ☑ Dart/Zebra
☑ ISO ☑ IEEE
□ Tag ID
☑ Grid with spacing of 10 feet

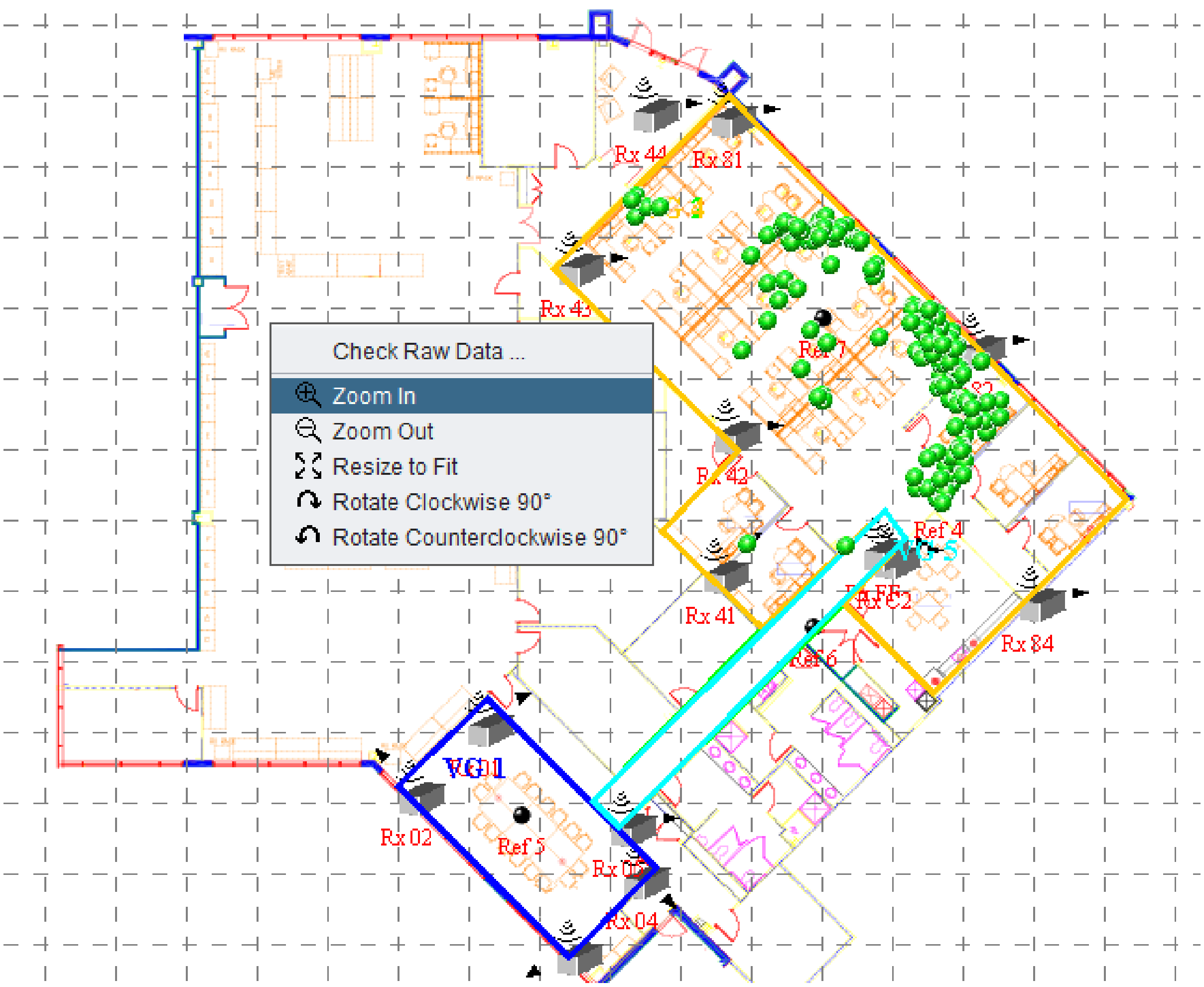
Search Tag [hide]

Tag ID:
Result:
Location:
Battery:
Last Seen:

Site Map

○ Default_Site
● Zebra_mssi_office
○ Zebra_mssi_lab

If required, right-click the map and select an option to zoom in or out, resize to fit, or rotate the map.



Viewing and filtering the raw data stream from the Hub

You can view, record, and filter the raw data stream of location data from the Hub.

To view and filter the raw data stream from the Hub:

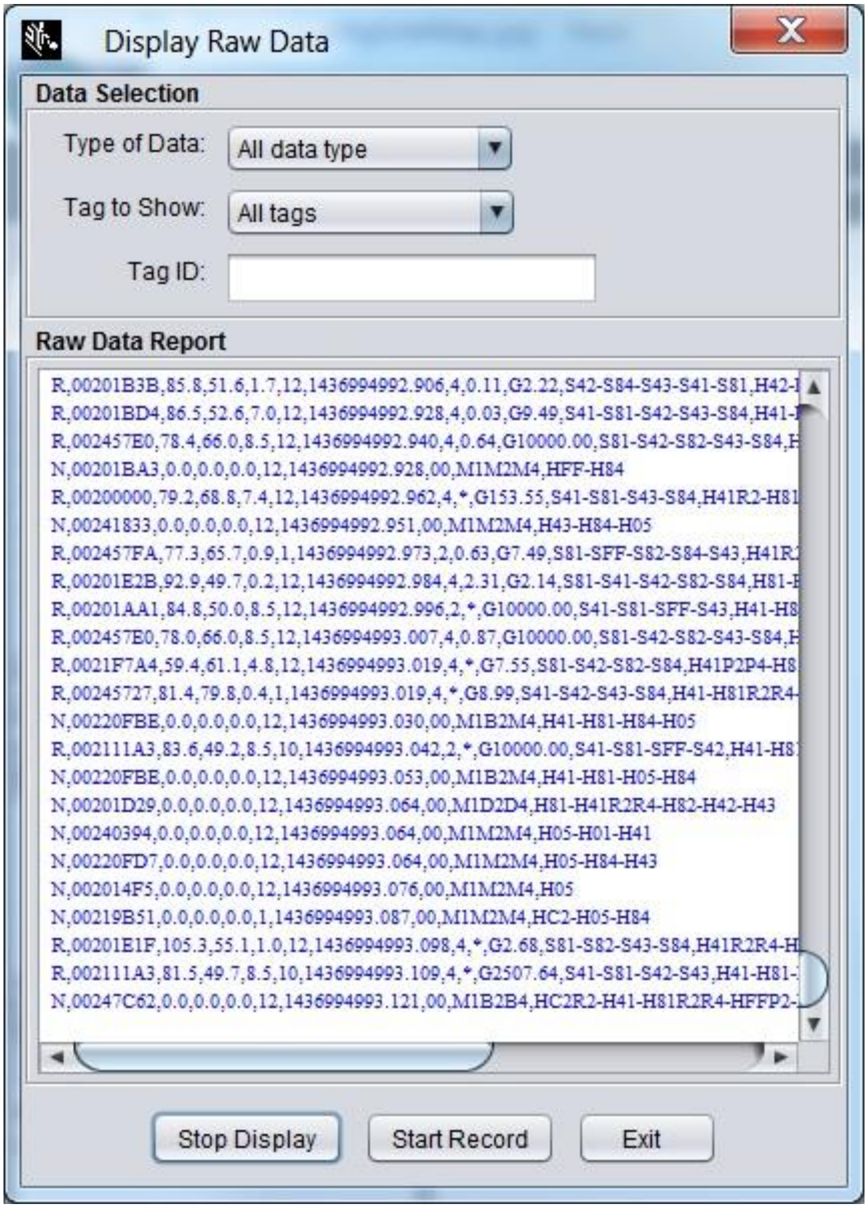
1 Start the **Hub Administration and Management** application, click **Demonstration**.

2 In the **Demonstration** view, right-click the map and select **Check Raw Data**.

3 In the **Display Raw Data** dialog box, under **Data Selection**, provide the following information:

- **Type of Data:** Select the data types to display, which can be **All**, **3D/2D/1D**, **3D/2D**, **3D**, **2D**, **1D**, **P/N**, or **Diagnostic**.

- **Tag to show:** Select whether to view data for all tags or for a specific tag. If you select **Specify a tag**, enter a Tag ID into the respective field.



Type of Data: All data type

Tag to Show: All tags

Tag ID:

```
R,00201B3B,85.8,51.6,1.7,12,1436994992.906,4,0.11,G2.22,S42-S84-S43-S41-S81,H42-
R,00201BD4,86.5,52.6,7.0,12,1436994992.928,4,0.03,G9.49,S41-S81-S42-S43-S84,H41-
R,002457E0,78.4,66.0,8.5,12,1436994992.940,4,0.64,G10000.00,S81-S42-S82-S43-S84,H
N,00201BA3,0.0,0.0,0.0,12,1436994992.928,00,M1M2M4,HFF-H84
R,00200000,79.2,68.8,7.4,12,1436994992.962,4,*,G153.55,S41-S81-S43-S84,H41R2-H81
N,00241833,0.0,0.0,0.0,12,1436994992.951,00,M1M2M4,H43-H84-H05
R,002457FA,77.3,65.7,0.9,1,1436994992.973,2,0.63,G7.49,S81-SFF-S82-S84-S43,H41R
R,00201E2B,92.9,49.7,0.2,12,1436994992.984,4,2.31,G2.14,S81-S41-S42-S82-S84,H81-
R,00201AA1,84.8,50.0,8.5,12,1436994992.996,2,*,G10000.00,S41-S81-SFF-S43,H41-H8
R,002457E0,78.0,66.0,8.5,12,1436994993.007,4,0.87,G10000.00,S81-S42-S82-S43-S84,H
R,0021F7A4,59.4,61.1,4.8,12,1436994993.019,4,*,G7.55,S81-S42-S82-S84,H41P2P4-H8
R,00245727,81.4,79.8,0.4,1,1436994993.019,4,*,G8.99,S41-S42-S43-S84,H41-H81R2R4-
N,00220FBE,0.0,0.0,0.0,12,1436994993.030,00,M1B2M4,H41-H81-H84-H05
R,002111A3,83.6,49.2,8.5,10,1436994993.042,2,*,G10000.00,S41-S81-SFF-S42,H41-H8
N,00220FBE,0.0,0.0,0.0,12,1436994993.053,00,M1B2M4,H41-H81-H05-H84
N,00201D29,0.0,0.0,0.0,12,1436994993.064,00,M1D2D4,H81-H41R2R4-H82-H42-H43
N,00240394,0.0,0.0,0.0,12,1436994993.064,00,M1M2M4,H05-H01-H41
N,00220FD7,0.0,0.0,0.0,12,1436994993.064,00,M1M2M4,H05-H84-H43
N,002014F5,0.0,0.0,0.0,12,1436994993.076,00,M1M2M4,H05
N,00219B51,0.0,0.0,0.0,1,1436994993.087,00,M1M2M4,HC2-H05-H84
R,00201E1F,105.3,55.1,1.0,12,1436994993.098,4,*,G2.68,S81-S82-S43-S84,H41R2R4-H
R,002111A3,81.5,49.7,8.5,10,1436994993.109,4,*,G2507.64,S41-S81-S42-S43,H41-H81-
N,00247C62,0.0,0.0,0.0,12,1436994993.121,00,M1B2B4,HC2R2-H41-H81R2R4-HFFP2-
```

Under **Raw Data Report**, you can:

- Control the output flow of Hub data to this display, by selecting **Stop Display** or **Start Display**.
- Record the raw data stream to a text file by selecting **Start Record**.   When prompted, enter a file name for saving the logged data.
- To stop recording entirely, click **Stop Record**.

Click **Exit** to close the dialog box.

Changing the site map

You can change the site map of the 2-D grid that displays the graphical results by adding customized background files to the Hub. Map files must be in `.jpg`, `.gif`, `.emf` or `.wmf` format.

To change the site map:

1 Start the **Hub Administration and Management** application, click **Configuration**.

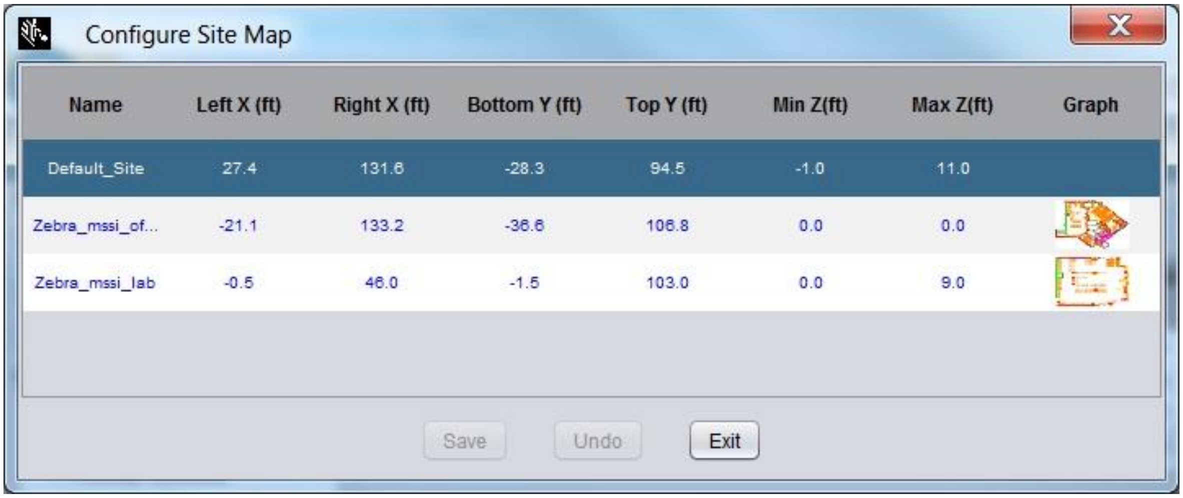
2 In the **Configuration** view, click **Configure Site Map**.

3 In the **Configure Site Map** dialog box, provide the following information for all maps to be used by the Hub:

- **Name:** Enter a name for the map. Dart RTLS uses this information for storing the image to the Hub.
- **Left X, Right X:** Enter the X coordinates for the corners of the map.
- **Bottom Y, Upper Y:** Enter the Y coordinates for the corners of the map.
- **MinZ, MaxZ:** Enter the Z coordinates for the minimum and maximum heights to be displayed on the map.
- **Graph:** Double-click to identify the location of the site map; browse to locate the map to be stored on the Hub.

> To create a new map or delete a map, right-click a row and select **Add** or **Remove**.

4 Click **Save**; then click **Exit**.



Configure Site Map

Name	Left X (ft)	Right X (ft)	Bottom Y (ft)	Top Y (ft)	Min Z(ft)	Max Z(ft)	Graph
Default_Site	27.4	131.6	-28.3	94.5	-1.0	11.0	
Zebra_mssi_of...	-21.1	133.2	-36.6	106.8	0.0	0.0	
Zebra_mssi_lab	-0.5	46.0	-1.5	103.0	0.0	9.0	

11 System output

Dart RTLS system provides different outputs format options, Dart and Z-SLMF, which are supported on TCP ports 5117and 5118 respectively. All tag data from the Dart hub, are coded in ASCII and sent over the LAN interface. To retrieve tag data from the Hub, you need a client program using the stream communication protocol and a connection to the output port. This section describes the format of tag data in the Dart output data stream

In This Section

Basic system output

The format of tag location output is as follows:

`<Data Header>,<tag >,<X>,<Y>,<Z>,<battery>,<timestamp>,<unit><LF>`

Where:

- **`<Data Header>`** represents the tag dimensional information. It can take on the following values:
  - `R`: 3-D calculation valid for X, Y, and Z (R-packet). 3-D calculations require four or more non-coplanar Receivers to detect an event and for software computations to complete successfully.
  - `T`: 2-D calculation valid for X and Y (T-packet). 2-D calculations occur when three Receivers respond and the software is able to compute the X and Y locations. The Z value is estimated to be the average heights of associated Receivers.
  - `O`: 1-D estimated calculation for X and Y (O-packet). This can occur in the event of only 2 Receivers responding such that the software estimates the tag position to be at an intermediate point along the line connecting the Receivers.
  - `P`: Presence indicator (P-Packet). This indicates that a Receiver detected a tag. Presence indicator data may be sent only when the Presence Detection flag is set for the RTLS Receiver, and when less than Min_unit number of Receivers are heard (that is not

enough information is available to calculate the position), or 1-, 2-, or 3-D calculations are unsuccessful. You also use P-packets to show data from a Proximity Receiver.

- `N`: Extended Non-locate packet (N-Packet). N packets give extended information for a non-locate 'P' packet. N packets contain the detect details and when enabled, are sent instead of the non-locate P packets.
- `D`: Diagnostic packet (D-packet). D packets are optional error and/or warning messages that are useful both during initial installation and for continuous monitoring of Dart RTLS. For a complete description of D-packets, see ***D-packets*** (on page 107).

- **`<tag#>`** is the tag ID.
- **`<X>`**, **`<Y>`**, **`<Z>`**, except for "P" type data, are the calculated tag coordinates in feet or meters with respect to a user-supplied origin, for R, T, and O type of data. In the case of P type of data, `<X>`, `<Y>`, `<Z>` represents the coordinates of the Receiver that detect this tag message transmission.
- **`<battery>`** is the tag's battery indicator. The value is a number between 0 and 15, where 15 represents a fully charged battery. The battery value is not linear, nor is the curve the same across all kinds of tags. The following table should be used to identify battery low condition on a particular tag.

Tag ID Format	Tag ID Range	Battery Level	Battery Status
IEEE / ISO	all	12	Good
IEEE / ISO	all	1	Low
Dart	00000001 - 00007FFF	10 - 15	Good
Dart	00000001 - 00007FFF	0 - 9	Low
Dart	00008000 - 001FFFFF	3 - 15	Good
Dart	00008000 - 001FFFFF	0 - 2	Low
Dart	00210000 - 00217FFF	10 - 15	Good
Dart	00210000 - 00217FFF	0 - 9	Low
Dart	00218000 - FFFFFFFF	12	Good
Dart	00218000 - FFFFFFFF	1	Low

- **`<timestamp>`** represents the Hub system time at which the data was processed. The format for timestamp is UNIX time, day, and year the data was computed. The value is in decimal and represents the number of elapsed seconds since January 1, 1970 UTC.

- **<unit>** except for P type data, is a Virtual Group ID (in decimal). The tag location data is computed from the time of flight measurements of the Receivers within the virtual group. In the case of P type data, `<unit>` is the Rx # of the Receiver that detected the transmission.
- **<LF>** is a Line Feed character (with ASCII code = 0x0A) to terminate a location data string.

The following is an example of system output from a Dart RTLS Hub.

```
T,0021F7B1,29.53,18.38,1.52,12,1433877485.930,4,*,G0.73,S81-S42-S82,H81-
HFF-H42-H82
N,00210EA1,0.00,0.00,0.00,10,1433877485.919,00,M1M2M4,HFF
N,00200015,0.00,0.00,0.00,12,1433877485.919,00,M1M2M4,H05
R,00210E2C,24.45,15.25,2.59,5,1433877485.942,4,*,G10000.00,S81-S42-S43-
S84,HFF-H81-H42-H43-H84P2
N,00201ADC,0.00,0.00,0.00,12,1433877485.942,00,M1C2B4,HC2R2-H05-H82-H43-
H84R2
T,00201BCD,26.68,15.04,1.01,12,1433877485.976,4,*,G10000.00,S41-S81-
S42,H41-H81-HFF-H42
O,00200012,31.99,5.04,2.59,12,1433877589.601,2,*,G*,S05-S84,H05-H84
N,00241732,0.00,0.00,0.00,12,1433877589.601,00,M1B2B4,H42-H82
N,00200013,0.00,0.00,0.00,12,1433877589.590,00,M1M2M4,H05
N,00211207,0.00,0.00,0.00,9,1433877589.590,00,M1M2M4,H05
N,002455DF,0.00,0.00,0.00,12,1433877589.590,00,M1M2M4,H82
N,00200E70,0.00,0.00,0.00,12,1433877589.601,00,M1M2M4,H42
N,00214C90,0.00,0.00,0.00,10,1433877589.601,00,R1M2M4,H01-H02-H04
N,00221B6C,0.00,0.00,0.00,12,1433877589.601,00,M1M2M4,H05
T,00201C40,25.85,15.67,2.59,12,1433877589.612,4,0.74,G0.42,S42-S82-S43-
S84-S81,H42-H82-H43-H84-H41P2P4-H81-HFF
O,00210F44,22.82,17.20,2.59,10,1433877589.646,4,*,G*,S81-S42,HC2P2-H81-
H05-H42R2
P,00210F51,18.44,-2.47,2.59,6,1433877589.646,05,P
T,0021117B,24.62,13.95,2.59,10,1433877589.669,4,1.55,G0.43,S41-S81-S42-
S82-S43,H41-H81-HFF-H42-H82-H43
N,00200013,0.00,0.00,0.00,12,1433877589.658,00,M1M2M4,H05
```

Data Quality Indicator (DQI)

If you have enabled Data Quality Indicator (DQI) (see ***Configuring output control*** (on page 43)), the output data appears in the following format, with an additional field `<DQI>`:

```
<Data Header>,<tag #>,<X>,<Y>,<Z>,<battery>,<timestamp>,<unit>,<DQI>,<LF>
```

Where `<DQI>` is the Data Quality Indicator value for the location data. When the DQI result is not meaningful this field contains an asterisk.

Geometric Dilution of Precision (GDOP)

Geometric Dilution of Precision (GDOP) is used to quantify the location accuracy of each blink based on the geometry of the receivers detecting the tag blink and the calculated location of the tag. If you have enabled Geometric Dilution of Precision (GDOP) (see ***Configuring output control*** (on page 43)), the output data appears in the following format, with an additional field `<GDOP>`:

```
<Data Header>,<tag #>,<X>,<Y>,<Z>,<battery>,<timestamp>,<unit>,<GDOP>,<LF>
```

Where <GDOP> is the Geometric Dilution of Precision value for the location data with prefix of 'G'. When the GDOP result is not meaningful this field contains an asterisk.

Non-locate Details

Non-locate details is an optional field that is available for the output data stream. This information helps assess why location data is not available for a particular tag event.

Non-locate details can take on the values described in the following table.

Value	Description
P	Only presence data expected. The **Receiver** is not part of a virtual group and is set up to provide only P data.
M<VG#>	Minimum units for the virtual group not met. For example, if the computation for minimum units is set to 3, then less than three Receivers detected this tag transmission.
B<VG#>	Bounding Box not met. The system computed the information, but the resulting coordinates were outside of the values defined for the ***Group Boundary*** (on page 36).
C<VG#>	Convergence not met. The system computed the information but failed to reach a convergence result.
R<VG#>	Reference is currently not available for virtual group computation. This may also indicate reference suspension failure when Presence Detection is configured.
G<VG#>	GDOP threshold value for the virtual group exceeded when filtering is enabled.
D<VG#>	DQI threshold value for the virtual group exceeded when filtering is enabled.

If you have enabled Non-locate details (see ***Configuring output control*** (on page 43)), the output P data appears in the following format, with an additional field `<Non-locate details>`:

```
P,<tag #>,<X>,<Y>,<Z>,<battery>,<timestamp>,<unit>,<Non-locate details><LF>
```

where `<Non-locate details>` is the reason for the P data output.

In the following example for system output from a Dart RTLS Hub, Min-units are not met:

```
P,0000099C,6.3,43.4,8.5,13,1162219029.404,A1,M1
P,0000099C,1.1,2.2,8.5,13,1162219029.404,11,M1
P,0000099C,99.8,43.4,8.2,13,1162219029.404,41,M1
```

In the following example, Receiver units 31 and 41 have detected tag 101616AD ; the Non-locate details (M1) indicates that a location computation was not made because virtual group 1 did not have enough Receivers to detect this tag event (minimum number of Receivers for VG1 was set to 3).

```
P,101616AD,100.0,15.4,8.5,11,1162219029.441,31,M1
P,101616AD,99.8,43.4,8.2,11,1162219029.441,41,M1
```

In the following example, Convergence is not met:

```
P,00002294,99.8,43.4,8.2,11,1161175614.527,D1,C1
P,00002294,6.3,43.4,8.5,12,1161175614.527,A1,C1
```

```
P,00002294,1.1,2.2,8.5,12,1161175614.527,B1,C1
```

In this example, Receiver units A1, B1, and D1 have detected tag 00002294; the Non-locate details (C1) indicates that a location computation was not made because virtual group 1 could not converge on a good location computation. This information likely means that one or more of the Receivers reporting tag 00002294 are getting an indirect signal (reflection) instead of a direct signal from the tag.

In the following example, VG1 has no reference and VG2 is outside of the bounding box:

```
P,0000099C,100.0,15.4,8.5,13,1161175614.363,C1,R1B2
P,0000099C,99.8,43.4,8.2,13,1161175614.363,D1,R1B2
P,0000099C,6.3,43.4,8.5,13,1161175614.363,A1,R1B2
P,0000099C,1.1,2.2,8.5,13,1161175614.363,B1,R1B2
```

In this example, the Receiver units A1, B1, C1, and D1 have detected tag 0000099C; the Non-locate details (R1B2) indicates that a location computation was not made because VG1 did not have a good reference tag signal and VG2 computed a position outside of the user-defined area for that virtual group.

N (Extended non-locate) packets

'N' packet give extended information for a 'P' (presence) packet for a non-locate. 'N' packets facilitate getting more information for a 'P' packet by including the detect details in addition to the non-locate details. Note: When 'N' packets are enabled, non-locates generate 'N' packets ***instead*** of 'P' packets.

The format of the 'N' packet is as follows :

N,<tag #>,0.0,0.0,0.0,<battery>,<timestamp>,00,<non-locate details>,<detect details><LF>

Example 1:

- *N,00210EA1,0.0,0.0,0.0,10,1433426937.852,00,M1M2M4,HFF-H42-H43P2-H84P2*
  - *M1M2M4* - non-locate details indicating minimum unit for the virtual groups 1, 2 and 4 were not met.
  - *HFF-H42* – receivers FF and 42 saw the blink and were not pruned or pre-pruned in any virtual groups.
  - *H43P2-H84P2* – receivers 43 and 84 saw the blink but were pre-pruned in virtual group 2.

Example 2:

- *N,A0002044,0.0,0.0,0.0,12,1433426937.874,00,M1B2B4,H41-H81-H42-H82R2R4-H43R2R4-H84*
  - *M1B2B4* - non-locate details indicating minimum unit not met for virtual group 1 and bounding box not met for virtual groups 2 and 4.
  - *H41-H81-H42--H84* – receivers 41, 81, 42 and 84 saw the blink and were not pruned or pre-pruned in any virtual groups.
  - *H82R2R4-H43R2R4* – receivers 82 and 43 saw the blink but were pruned out in virtual groups 2 and 4.

Locate Details

You can enable Locate details for the output data stream (see ***Configuring output control*** (on page 43)). Locate details TLS describes which Receivers were used in a location computation. The output appears in the following format, with an additional field `<Locate-Details>`:

```
<Data Header>,<tag #>,<X>,<Y>,<Z>,<battery>,<timestamp>,<unit>,<Locate-
Details><LF>
```

where `<Locate-Details>` describes the Receivers involved in the location computation. The following example for system output from a Dart RTLS Hub shows that the Receivers 37, 38, and 43 have detected tag ID 00200007 and involved in the location calculation:

```
T,00200007,46.2,32.2,0.0,13,1282704616.251,3,S37-S38-S43
T,00200007,46.2,32.2,0.0,13,1282704617.146,3,S37-S38-S43
T,00200007,46.2,32.2,0.0,13,1282704619.045,3,S37-S38-S43
T,00200007,46.2,32.2,0.0,13,1282704620.942,3,S37-S38-S43
```

Detail Details

The hub can be configured to output detect details which can be helpful for troubleshooting. Locates and non-locates will now contain details about receivers that detected the blinks, receivers that were pre-pruned and receivers that were pruned out.

With additional detect details, the data output has the format **H**rr[**P**xx][**R**yy] where

Hrr: indicates receiver rr saw the tag blink where rr is the receiver number

Pxx: indicates receiver rr was pre-pruned during tag location calculation in virtual group xx. **Pxx** may not appear if the receiver was not pre-pruned in any virtual group; it might appear multiple times if the receiver was pre-pruned in more than one virtual group.

Ryy: indicates receiver rr was pruned during tag location calculation in virtual group yy. **R**yy may not appear if pruning was turned off or receiver was not pruned in any virtual group; it might appear multiple times if the receiver was pruned in more than one virtual group.

In the below T (2D locate) packet examples, ‘S’ indicates the receivers that were used for the locate computation, ‘H’ indicates the receivers that detected the tag blink, ‘P’ indicates pre-pruning and ‘R indicates pruning.

Note – If a receiver is present in the ‘H’ list without ‘P’ or ‘R’ but not present in the ‘S’ list, that means that particular receiver saw the blink and was used for computation in a virtual group, but that virtual group computation was not selected for the final locate computation.

Example 1:

- *`T,00210EA1,81.9,47.2,5.0,10,1433424562.700,2,0.93,G0.62,SFF-S81-S42-S84,H41P2P4-HFF-H81-H42-H84-H43P2P4`*
    - SFF-S81-S42-S84 - receivers FF, 81, 42 and 84 were used for this locate computation.
    - H41P2P4- H43P2P4 – receiver 41 and 43 saw the blink but it was pruned in virtual group 2 and virtual group 4.
    - HFF-H81-H42-H84 – receivers FF, 81, 42 and 84 saw the blink and were not pruned or pre-pruned in any virtual groups.

Example 2:

- *`T,00201B47,81.1,47.7,5.0,12,1433424563.235,4,3.09,G0.34,S41-S81-S42-S82-S43-S84,HC2P2-H41-H81R2-HFF-H42-H82R2-H43-H84P2`*
    - S41-S81-S42-S82-S43-S84 – receivers 41, 81, 42, 82, 43 and 84 were used for this locate computation.
    - HC2P2-H84P2 – receivers C2 and 84 saw the blink but were pre-pruned in virtual group 2.
    - H41-HFF-H42-H43 – receivers 41, FF, 42 and 43 saw the blink and were not pruned or pre-pruned in any virtual groups.
    - H81R2-H82R2 - receivers 81 and 82 saw the blink but were pruned in virtual group 2.

Example 3:

- *`T,002415AB,103.8,45.4,5.0,12,1433424574.154,4,0.11,G0.97,S42-S43-S84-S41,H05-H42-H82R2R4-H43-H84-HC2P2-H41-H81P4R2`*
    - S42-S43-S84-S41 - receivers 42, 43, 84 and 41 were used for this locate computation.
    - H05-H42-H43-H84-H41 – receivers 5,42,43,84 and 41 saw the blink and were not pruned or pre-pruned in any virtual groups.
    - H82R2R4 – receiver 82 saw the blink but was pruned out in virtual groups 2 and 4.
    - HC2P2 – receiver C2 saw the blink but was pre-pruned in virtual group 2.
    - H81P4R2 – receiver 81 saw the blink but was pre-pruned in virtual group 4 and pruned out in virtual group 2.

12 Diagnostics

Dart RTLS provides low-level tests that you can use to determine the receive range of each active Receiver.

For example, you can detect:

- Whether a reference signal is in a good position for all Receivers within a reference group.
- Whether a particular Receiver is receiving tag transmissions adequately.
- What Receivers are detecting a tag (possibly in error, due to reflections).
- Cabling problems with connections to Receivers.

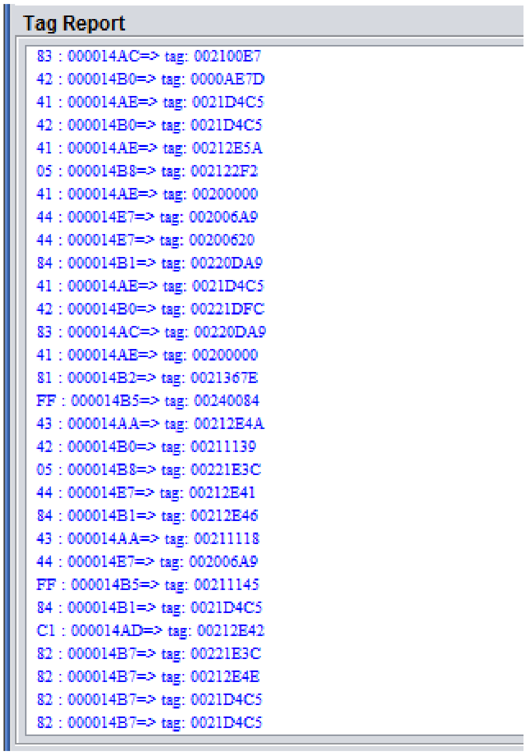
Diagnostic testing interrupts normal system operation.

In This Section

Receiver test

With the Receiver Test, you can:

- Examine the real-time data collection of tag information (**Tag Report** field), as illustrated in the figure. Information is presented as `Rx #: Receiver ID => tag: tag ID`.



```
83 : 000014AC=> tag: 002100E7
42 : 000014B0=> tag: 0000AE7D
41 : 000014AE=> tag: 0021D4C5
42 : 000014B0=> tag: 0021D4C5
41 : 000014AE=> tag: 00212E5A
05 : 000014B8=> tag: 002122F2
41 : 000014AE=> tag: 00200000
44 : 000014E7=> tag: 002006A9
44 : 000014E7=> tag: 00200620
84 : 000014B1=> tag: 00220DA9
41 : 000014AE=> tag: 0021D4C5
42 : 000014B0=> tag: 00221DFC
83 : 000014AC=> tag: 00220DA9
41 : 000014AE=> tag: 00200000
81 : 000014B2=> tag: 0021367E
FF : 000014B5=> tag: 00240084
43 : 000014AA=> tag: 00212E4A
42 : 000014B0=> tag: 00211139
05 : 000014B8=> tag: 00221E3C
44 : 000014E7=> tag: 00212E41
84 : 000014B1=> tag: 00212E46
43 : 000014AA=> tag: 00211118
44 : 000014E7=> tag: 002006A9
FF : 000014B5=> tag: 00211145
84 : 000014B1=> tag: 0021D4C5
C1 : 000014AD=> tag: 00212E42
82 : 000014B7=> tag: 00221E3C
82 : 000014B7=> tag: 00212E4E
82 : 000014B7=> tag: 0021D4C5
82 : 000014B7=> tag: 0021D4C5
```

- Run a timed test to get a list of all tags that a Receiver detects (**Result** field). The test results in accumulated tag data per Receiver, showing the total number of good or missing tag packets per Receiver along with the calculated transmit frequency for each detected tag. The summary data also shows the total number of good packets and total tags detected per Receiver. For example:

```
Rx #A4 detected the following tags:
#0000448E => good/missing packets = 4/0; f = 0.79 Hz
#AABBCCDD => good/missing packets = 4/0; f = 0.79 Hz
#0000099C => good/missing packets = 4/0; f = 0.79 Hz
#00000B29 => good/missing packets = 3/0; f = 0.59 Hz
#00000B5D => good/missing packets = 4/0; f = 0.79 Hz
#0000274A => good/missing packets = 4/0; f = 0.79 Hz
#00005CAF => good/missing packets = 4/0; f = 0.79 Hz
#00000101 => good/missing packets = 4/0; f = 0.79 Hz
#000021BC => good/missing packets = 4/0; f = 0.79 Hz
#AABBCCEE => good/missing packets = 4/0; f = 0.79 Hz
#00005C33 => good/missing packets = 4/0; f = 0.79 Hz
#0000265C => good/missing packets = 4/0; f = 0.79 Hz
#0000760F => good/missing packets = 3/0; f = 0.59 Hz
#00000B3C => good/missing packets = 3/0; f = 0.59 Hz
#00002294 => good/missing packets = 3/0; f = 0.59 Hz
#00000D60 => good/missing packets = 3/0; f = 0.59 Hz
#00000500 => good/missing packets = 3/0; f = 0.59 Hz
#00000B48 => good/missing packets = 3/0; f = 0.59 Hz
Total good packets = 65; f = 12.85 Hz.
```

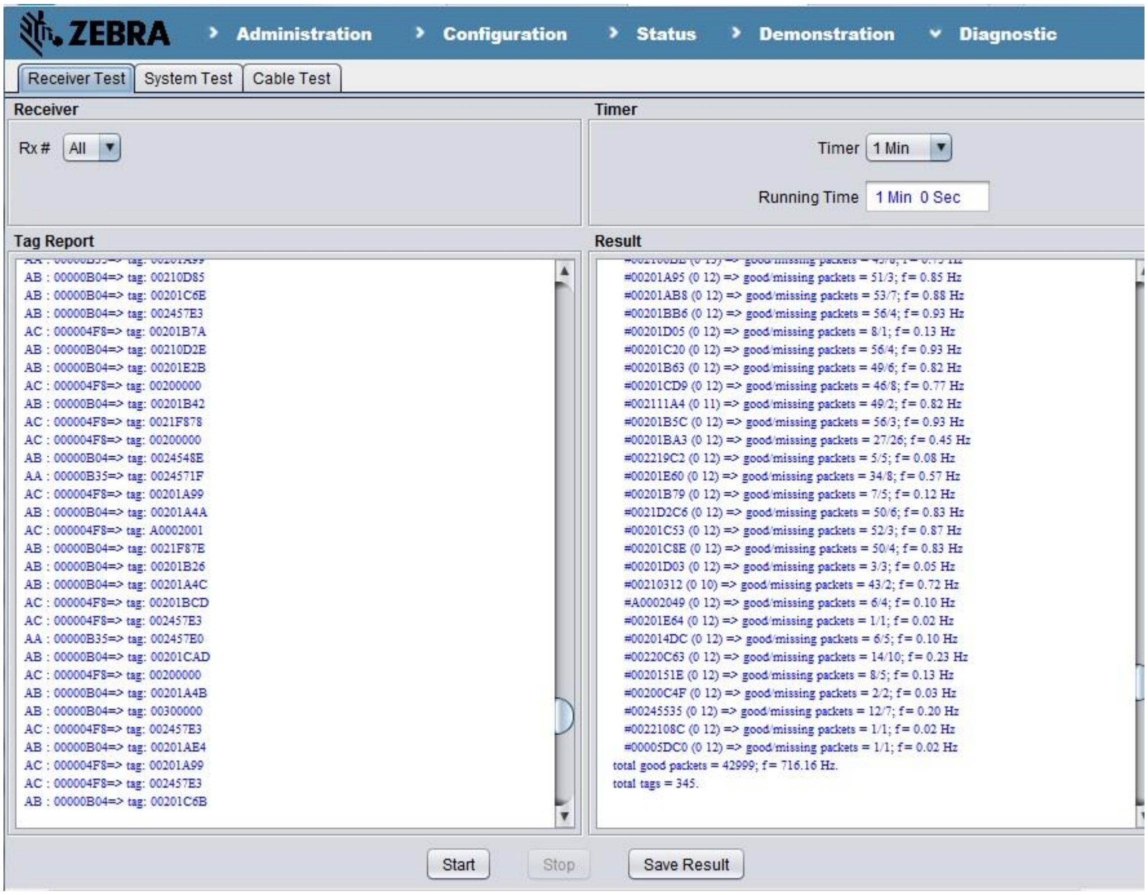
```
    Total tags = 18.
```

To run a timed test:

1 Start the **Hub Administration and Management** application, click **Diagnostics**.

2 In the **Diagnostics** view, on the **Receiver Test** tab, from the **Rx** # list inside **Receiver** section, select the receiver for which you want to run the test, or select **All** to include all receivers.

3 Optionally, from the **Timer** list in **Timer** section, select a particular time or select **Off**.



Rx # All

Timer 1 Min

Running Time 1 Min 0 Sec

```
AB : 00000B04=> tag: 00210D85
AB : 00000B04=> tag: 00201C6E
AB : 00000B04=> tag: 002457E3
AC : 000004F8=> tag: 00201B7A
AB : 00000B04=> tag: 00210D2E
AB : 00000B04=> tag: 00201E2B
AC : 000004F8=> tag: 00200000
AB : 00000B04=> tag: 00201B42
AC : 000004F8=> tag: 0021F878
AC : 000004F8=> tag: 00200000
AB : 00000B04=> tag: 0024548E
AA : 00000B35=> tag: 0024571F
AC : 000004F8=> tag: 00201A99
AB : 00000B04=> tag: 00201A4A
AC : 000004F8=> tag: A0002001
AB : 00000B04=> tag: 0021F87E
AB : 00000B04=> tag: 00201B26
AB : 00000B04=> tag: 00201A4C
AC : 000004F8=> tag: 00201BCD
AC : 000004F8=> tag: 002457E3
AA : 00000B35=> tag: 002457E0
AB : 00000B04=> tag: 00201CAD
AC : 000004F8=> tag: 00200000
AB : 00000B04=> tag: 00201A4B
AB : 00000B04=> tag: 00300000
AC : 000004F8=> tag: 002457E3
AB : 00000B04=> tag: 00201AE4
AC : 000004F8=> tag: 00201A99
AC : 000004F8=> tag: 002457E3
AB : 00000B04=> tag: 00201C6B
```

```
   #00201A95 (0 12) => good/missing packets = 51/3; f= 0.85 Hz
   #00201AB8 (0 12) => good/missing packets = 53/7; f= 0.88 Hz
   #00201BB6 (0 12) => good/missing packets = 56/4; f= 0.93 Hz
   #00201D05 (0 12) => good/missing packets = 8/1; f= 0.13 Hz
   #00201C20 (0 12) => good/missing packets = 56/4; f= 0.93 Hz
   #00201B63 (0 12) => good/missing packets = 49/6; f= 0.82 Hz
   #00201CD9 (0 12) => good/missing packets = 46/8; f= 0.77 Hz
   #002111A4 (0 11) => good/missing packets = 49/2; f= 0.82 Hz
   #00201B5C (0 12) => good/missing packets = 56/3; f= 0.93 Hz
   #00201BA3 (0 12) => good/missing packets = 27/26; f= 0.45 Hz
   #002219C2 (0 12) => good/missing packets = 5/5; f= 0.08 Hz
   #00201E60 (0 12) => good/missing packets = 34/8; f= 0.57 Hz
   #00201B79 (0 12) => good/missing packets = 7/5; f= 0.12 Hz
   #0021D2C6 (0 12) => good/missing packets = 50/6; f= 0.83 Hz
   #00201C53 (0 12) => good/missing packets = 52/3; f= 0.87 Hz
   #00201C8E (0 12) => good/missing packets = 50/4; f= 0.83 Hz
   #00201D03 (0 12) => good/missing packets = 3/3; f= 0.05 Hz
   #00210312 (0 10) => good/missing packets = 43/2; f= 0.72 Hz
   #A0002049 (0 12) => good/missing packets = 6/4; f= 0.10 Hz
   #00201E64 (0 12) => good/missing packets = 1/1; f= 0.02 Hz
   #002014DC (0 12) => good/missing packets = 6/5; f= 0.10 Hz
   #00220C63 (0 12) => good/missing packets = 14/10; f= 0.23 Hz
   #0020151E (0 12) => good/missing packets = 8/5; f= 0.13 Hz
   #00200C4F (0 12) => good/missing packets = 2/2; f= 0.03 Hz
   #00245535 (0 12) => good/missing packets = 12/7; f= 0.20 Hz
   #0022108C (0 12) => good/missing packets = 1/1; f= 0.02 Hz
   #00005DC0 (0 12) => good/missing packets = 1/1; f= 0.02 Hz
total good packets = 42999; f= 716.16 Hz.
total tags = 345.
```

4 Click **Start** to run the test.

5 When the test is done, click **Save Results** to save the information to a text file for later reference

System test

The System Test helps you validate that the timing for computations of all enabled virtual groups is complete. It provides statistics about detected receivers and tags and lets you determine optimal receiver and reference tag groupings based on received transmissions from specified UWB tags.

Similar to the ***Receiver test*** (on page 91), you can time the System test or run it manually.

The System test reports information on:

- Reference tags: Shows the average tag reception rates for each receiver.
- RTLS receivers: Identifies timing consistencies and inconsistencies based on reference tag

grouping and average tag reception rates. The Hub software lists inconsistencies as *islands* within a virtual group.

- Battery status of Reference tags: Shows the battery level and indicates if the battery is low.

You can control the following System test parameters:

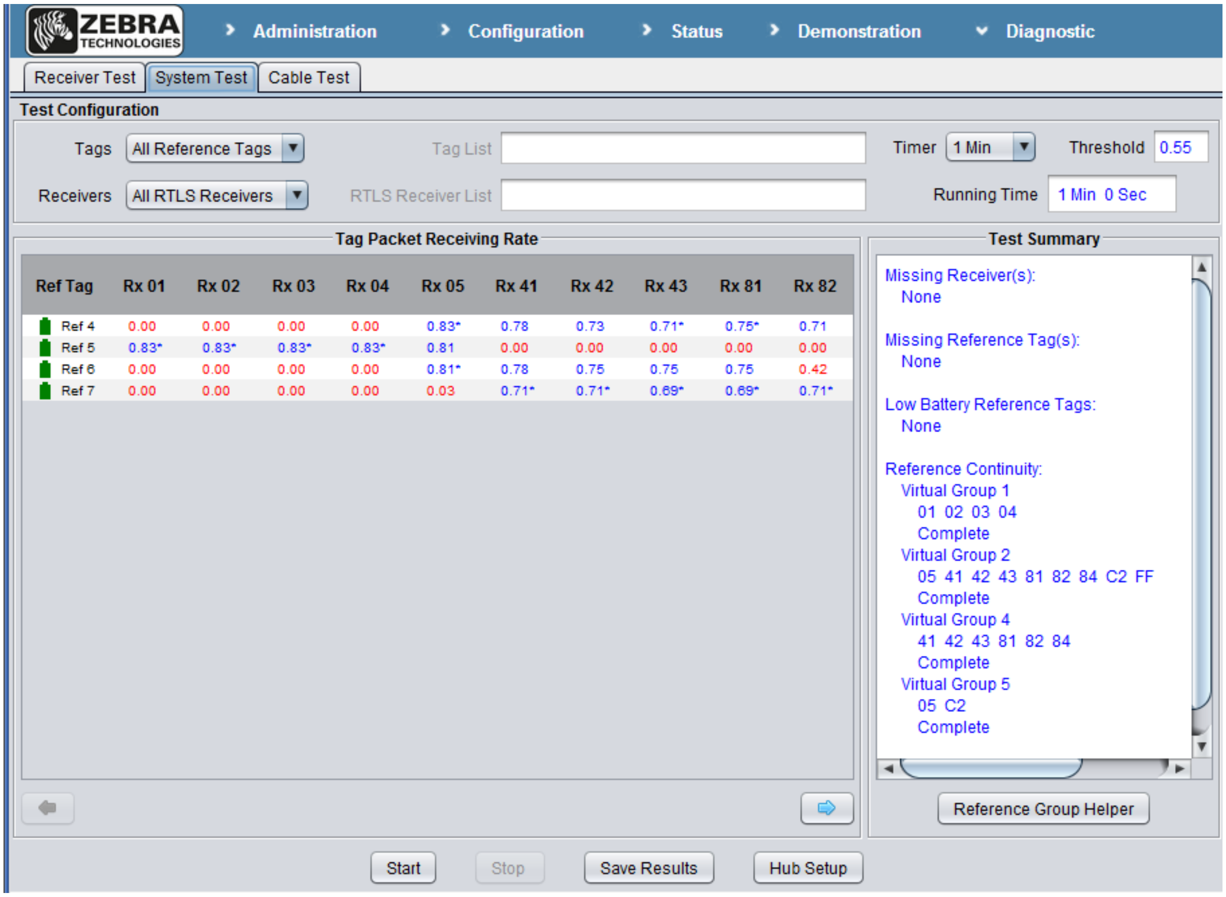
- **Tags:** Select **All Reference Tags**, **Tag List or All Tags** to determine what rate of tags each Receiver detects.
- **Receivers:** Select **All RTLS Receivers**, a specific RTLS Receiver List, or a Receiver List associated with a specific virtual group.
- **Timer:** Set a time (15, 30, or 60 seconds) or turn off to allow an un-timed test. You use the **Start** and **Stop** buttons to initiate or halt a test.
- **Threshold:** Set the value for good and bad receive rates for reference tags.

To run a timed test:

1 Start the **Hub Administration and Management** application, click **Diagnostics**.

2 In the **Diagnostics** view, on the **System Test** tab, from the **Tags** and **Receivers** lists, select the reference tags and receivers for which you want to run the test.

3 Optionally, from the **Timer** list, select a time or select **Off**.



Test Configuration

Tags: All Reference Tags

Tag List:

Timer: 1 Min

Threshold: 0.55

Receivers: All RTLS Receivers

RTLS Receiver List:

Running Time: 1 Min 0 Sec

Tag Packet Receiving Rate

Ref Tag	Rx 01	Rx 02	Rx 03	Rx 04	Rx 05	Rx 41	Rx 42	Rx 43	Rx 81	Rx 82
Ref 4	0.00	0.00	0.00	0.00	0.83*	0.78	0.73	0.71*	0.75*	0.71
Ref 5	0.83*	0.83*	0.83*	0.83*	0.81	0.00	0.00	0.00	0.00	0.00
Ref 6	0.00	0.00	0.00	0.00	0.81*	0.78	0.75	0.75	0.75	0.42
Ref 7	0.00	0.00	0.00	0.00	0.03	0.71*	0.71*	0.69*	0.69*	0.71*

Test Summary

Missing Receiver(s):
None

Missing Reference Tag(s):
None

Low Battery Reference Tags:
None

Reference Continuity:
Virtual Group 1
01 02 03 04
Complete
Virtual Group 2
05 41 42 43 81 82 84 C2 FF
Complete
Virtual Group 4
41 42 43 81 82 84
Complete
Virtual Group 5
05 C2
Complete

4 Click **Start** to run the test.

5 When the test is done, click **Save Results** to save the information to a text file for later reference.

6 Interpret the test results

- Under **Tag Packet Receiving Rate**:

  Examine the reference tags or tags in the **Ref Tag** or **Tag ID** field. If a reference tag is not detected, it is shown in red. Also check the battery icon ▮, which indicates the battery status of the reference tag. Green signals a good status, red icon ▯ means that the battery is low and you should replace the tag.

  Examine the **Rx** # columns, which display the average receive rate of the tag over the test time. Good practice is to use 1 Hz reference tags. Recommended reference tags have a detection frequency of 0.55 Hz or greater.

An asterisk (*) indicates that a receiver is included in a respective reference group.

- Under **Test Summary**:

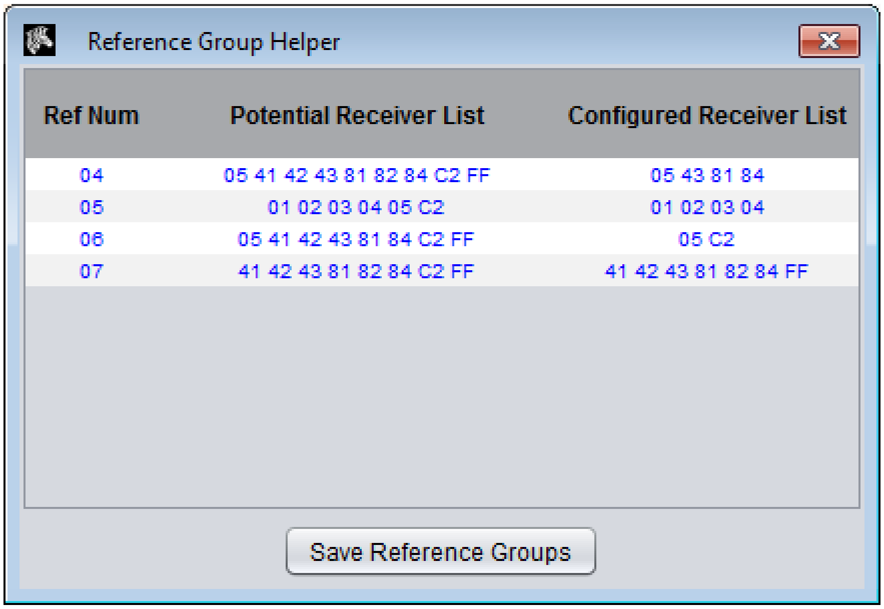
  Missing Receiver(s) lists Receivers under test that the Hub does not detect.

  Missing Reference Tags lists reference tags under test that are not detected by any Receivers under test.

  Low Battery Reference Tags lists all reference tags under test that are running out of battery. You need to replace those tags soon.

  Reference Continuity summarizes timing consistency per virtual group. To achieve complete continuity, reconfigure virtual groups with islands.

- Click **Reference Group Helper** to view a list of receivers that are a good match for a particular reference tag. This information summarizes the best reference tag–Receiver matches



Ref Num	Potential Receiver List	Configured Receiver List
04	05 41 42 43 81 82 84 C2 FF	05 43 81 84
05	01 02 03 04 05 C2	01 02 03 04
06	05 41 42 43 81 84 C2 FF	05 C2
07	41 42 43 81 82 84 C2 FF	41 42 43 81 82 84 FF

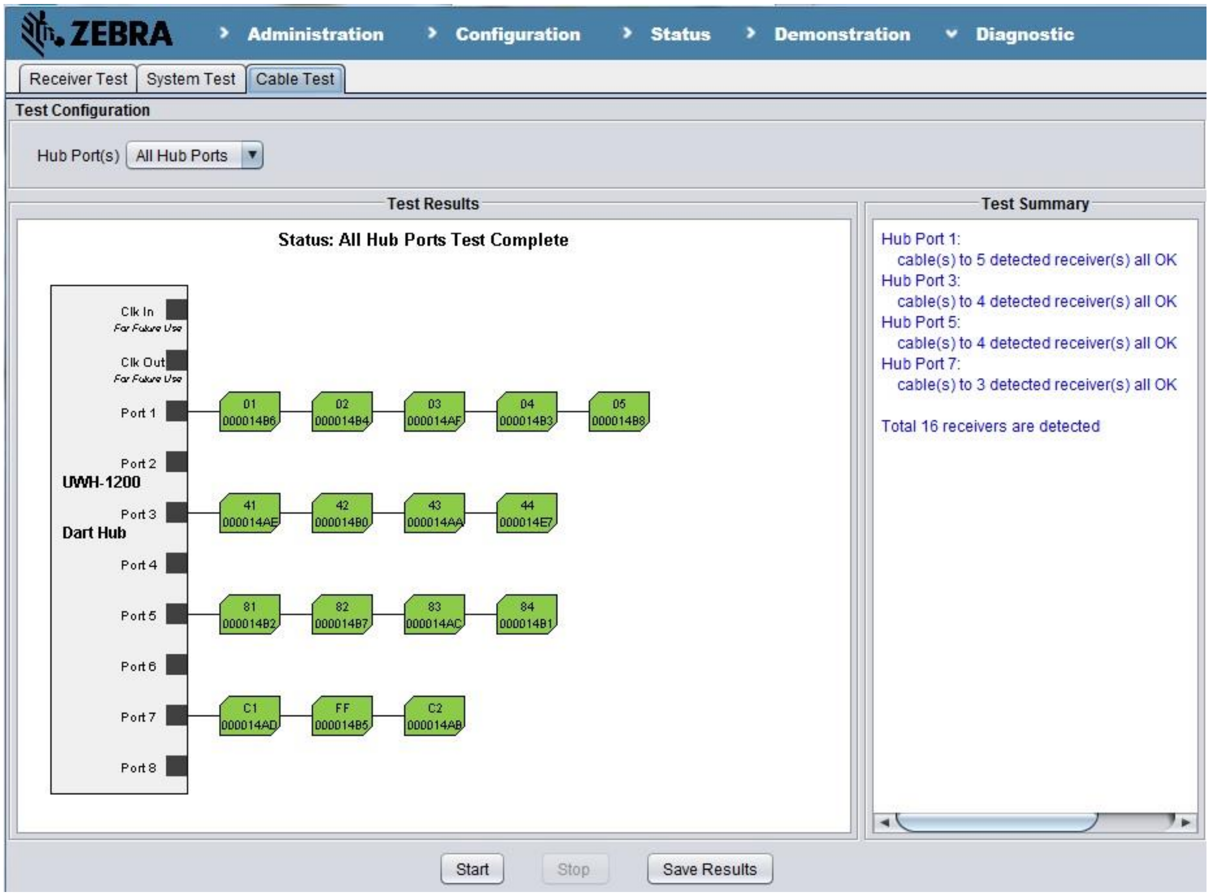
Cable Test

The Cable Test helps you to isolate defect(s) in cabling between Dart receivers and the hub.

To run a Cable Test:

1 Start the **Hub Administration and Management** application, click **Diagnostics**.

2 In the **Diagnostics** view, on the **Cable Test** tab, from the **Hub Port(s)** list, specify the hub port or all hub ports.



Hub Port(s) All Hub Ports

Status: All Hub Ports Test Complete

Hub Port 1:
cable(s) to 5 detected receiver(s) all OK
Hub Port 3:
cable(s) to 4 detected receiver(s) all OK
Hub Port 5:
cable(s) to 4 detected receiver(s) all OK
Hub Port 7:
cable(s) to 3 detected receiver(s) all OK

Total 16 receivers are detected

3 Click **Start** to run the test**.**

4 After start, on each selected hub port, the system detects receiver one by one. Whenever a new receiver is detected, a communication test is performed between the hub and that receiver, and the statistics on error(s) are collected. Each receiver is represented as a box and appended to the daisy chain after testing on that receiver connection completes. The fill-in color indicates the condition of the cable section connecting to the previous receiver or the hub port:

> **Green:** cable connection is good. **Yellow:** cable connection is not good but acceptable (<5% errors were detected in the communication test). Further check and replacement is recommended
>
> **Red:** cable connection is bad. Further check and replacement is needed.
>
> **Note:** Cable test is performed only on local receivers and not on remote receivers.

5 When the test is complete, click **Save Results** to save the test results to a text file for later reference.

For best results, receiver models of "AB" or better are required. Dart receiver of model "AB" or higher can provide loopbacks within the receiver. This loopback is useful in isolating where the cable fault is within a daisy chain. This test provides guidance on the locations of potentially poor cable connections. Some connection errors (such as termination errors on the power line of the cable) may be exhibited further downstream. In this case, additional debug with physical cable testers or cable replacement will be needed.

13 Status

You can use the Status view to examine the current status of the system and verify the proper operation of reference tags and Receivers. All status information updates every 10 seconds.

This Section

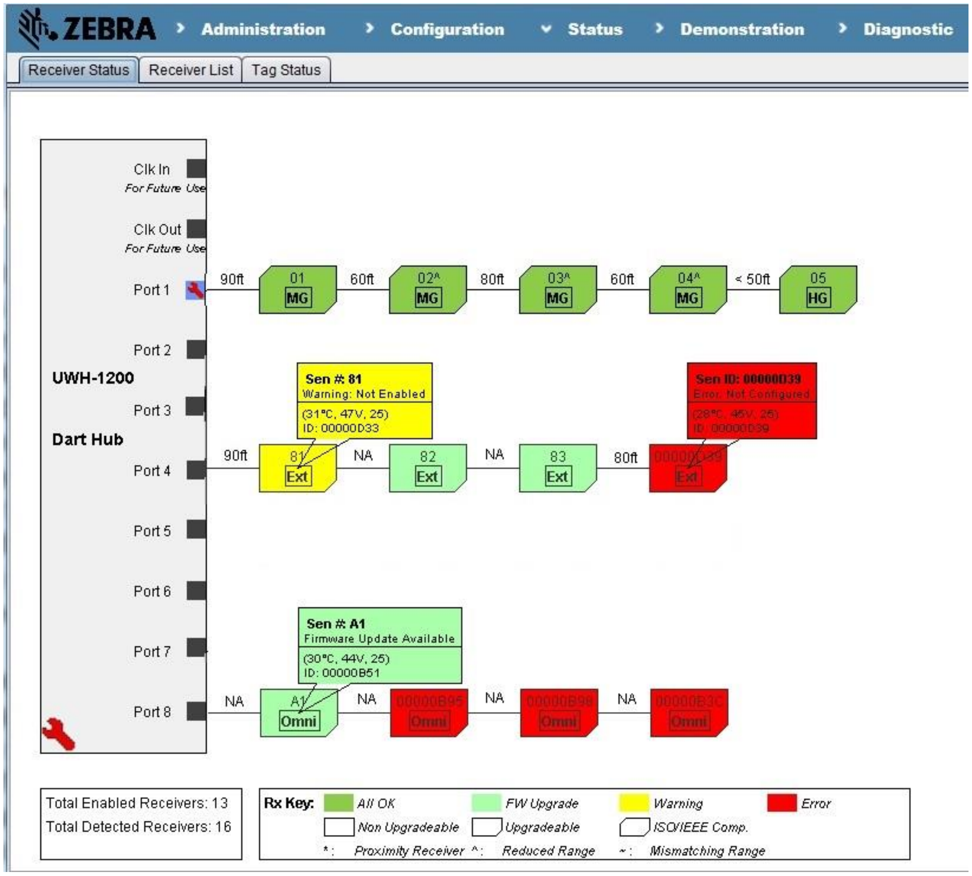
Viewing Receiver status

The **Receiver Status** tab shows information about the connections between each of the eight hub ports and the Receivers.

To view Receiver status:

1 Start the **Hub Administration and Management** application, click **Status.**

2 On the **Receiver Status** tab, examine the displayed information. This information automatically refreshes every 5 seconds.



Sen #: 81
Warning: Not Enabled
(31°C, 47V, 25)
ID: 00000D33

Sen ID: 00000D39
Error: Not Configured
(28°C, 45V, 25)
ID: 00000D39

Sen #: A1
Firmware Update Available
(30°C, 44V, 25)
ID: 00000B51

Total Enabled Receivers: 13
Total Detected Receivers: 16

Rx Key: 🟩 *All OK* 🟩 *FW Upgrade* 🟨 *Warning* 🟥 *Error*
□ *Non Upgradeable* □ *Upgradeable* □ *ISO/IEEE Comp.*
* : *Proximity Receiver* ^ : *Reduced Range* ~ : *Mismatching Range*

The tab displays the UWH-1200 hub and Receiver daisy chains connected to each hub port. Receivers are drawn in different rectangular box shapes, depending on their capability:

- A rectangular icon, 41 MG, represents a Receiver that does not support firmware upgrade;
- A rectangular icon with the bottom-right corner missing, 83 Ext, represents a receiver compatible with firmware upgrades;
- A rectangular icon with the bottom-right and upper-left corner missing, 02 MG, represents a receiver compatible with ISO/IEEE formatted tags.

The Dart Hub real time detects the receiver connections and displays visually in the right order on each port. Dart hub also measures the length of the cable between hub and receiver and between adjacent receivers if the receiver firmware (version 5.3.1 and above) and hub FPGA firmware (version 1.1.2 and above) support cable length measurement. The cable length is displayed section wise along with the units of measurement, rounded off to the nearest ten. Dart hub also continuously collects receiver status and updates them on the status page.

The connection order and cable length cannot be obtained for Remote Receivers and they are displayed in random order, on the port labelled ‘Remote’.

When a potential cable defect, such as loss of input clock at a receiver, is detected on a daisy chain, the maintenance icon 🔧 is painted on the corresponding port. In this case, a diagnostic Cable Test is recommended for this hub port. This maintenance alert will be cleared on Dart RTLS firmware restart.

In the unlikely event that UWH-1200 has to auto reboot to recover from a system fault, a

visual notification of a large maintenance icon 🔧 is shown at bottom-left corner of UWH-1200 Dart Hub. This notification can only be cleared by rebooting UWH-1200 hub.
In case of auto recovery from system fault, care has been take in Dart RTLS firmware so that reference timing established before system fault is preserved, and will be used after auto recovery.

The port is color coded either grey or blue representing the port speed. When blue, it indicates that all the receivers on that port support faster communication speed and so the port is in 4M bit/sec. The default speed is 2M bit/sec and the port operating at the default rate is colored grey.

Dart Hub monitors the CPU temperature by periodically reading it. If the CPU gets over-heated (temperature above 85 C), then an over-heat icon 🔥 is displayed on the bottom-left corner of the UWH-1200 Dart Hub.

Detected Receivers are color-coded to indicate the Receiver status. The color code used is listed in the **Key** box at bottom of the window:

- **Green:** The Receiver, like Receiver #01 on hub port 3, is fully operational; no warnings exist.
- **Light Green:** The Receiver, such as Receiver #A1 on hub port 8, is fully operational; receiver firmware upgrade is available.
- **Yellow:** The Receiver is operational, but warnings persist. For example, Receiver 81 connecting to hub port 5 is in yellow because it is not enabled for RTLS operation.
- **Red:** The Receiver is currently not operational; alarms persist. For example, Receiver 00000D39 is in red since it is not configured.

Each Receiver icon includes the number assigned to the Receiver and the Antenna type, which can be any of the following:

- **HG:** High gain antenna
- **MG**: Mid gain antenna
- **Omni**: Omni-directional antenna
- **Ext:** External antenna, typically due to use of a bulk head Receiver to connect the Receiver to an external or remote UWB antenna.
- **RR:** Receiver Repeater. A Receiver Repeater does not have antenna installed and it is used to extend the cable reach where cable lengths greater than 1000′ are needed.

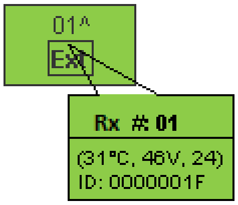
Each Receiver icon contains additional information including:

- **Temperature** (in Celsius)
- **Voltage** level
- Receiver **Read Range**
- **ID** (the unique 4-byte serial number on the back plate of the receiver)

The status of receiver read range is coded as a special character and appended to the receiver # in the receiver icon.

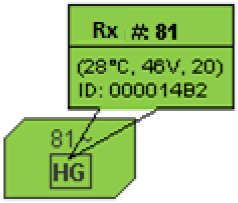
- **Reduced read range** A special character **'^'** is appended if the receiver has read range less than the maximum (25 in coarse range control mode or 54 in fine range control mode).

  In the following example, the Receiver #01 has an External antenna that is set at a read range setting of "24".



- **Mismatched read range:** A special character '~' is appended if the receiver has different read range setting than configured. This condition should not happen in normal condition. You should contact the factory if this condition appears.

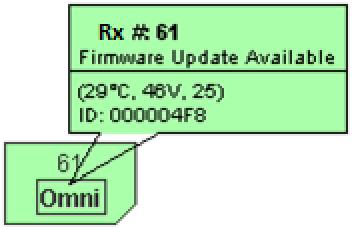
  In the following example, the Receiver #81 with a High-Gain antenna is reporting a read range setting not agreeing with its configured read range of "20".



3 Double-click on a Receiver rectangle to view more details about that receiver, such as:

- **Indication message (light green),** such as:

  Receiver firmware upgrade is available.

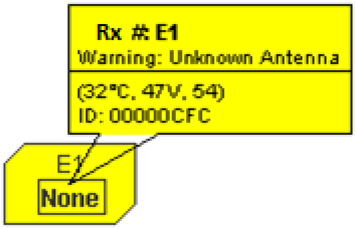


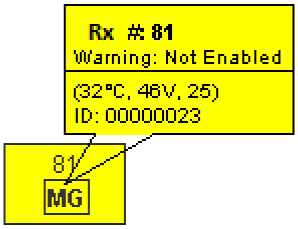
- **Warning message (yellow),** such as:

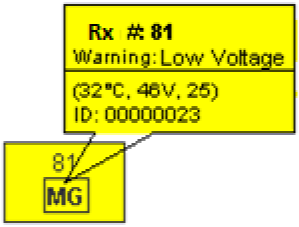
  Antenna type cannot be detected. Because a Receiver should be able to detect all antenna types, you should contact the factory if this message appears.

  Receiver is not enabled.

  Receiver has low voltage.


Rx # E1
Warning: Unknown Antenna
(32°C, 47V, 54)
ID: 00000CFC

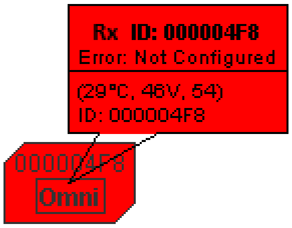

Rx # 81
Warning: Not Enabled
(32°C, 46V, 25)
ID: 00000023

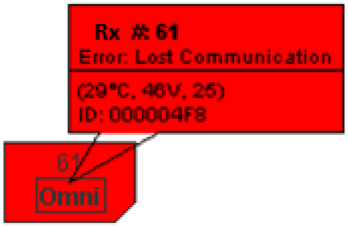

Rx # 81
Warning:Low Voltage
(32°C, 46V, 25)
ID: 00000023

- **Error message (red)**, such as:

  Receiver is not configured.

  Receiver communication loss.


Rx ID: 000004F8
Error: Not Configured
(29°C, 46V, 54)
ID: 000004F8


Rx # 61
Error: Lost Communication
(29°C, 46V, 25)
ID: 000004F8

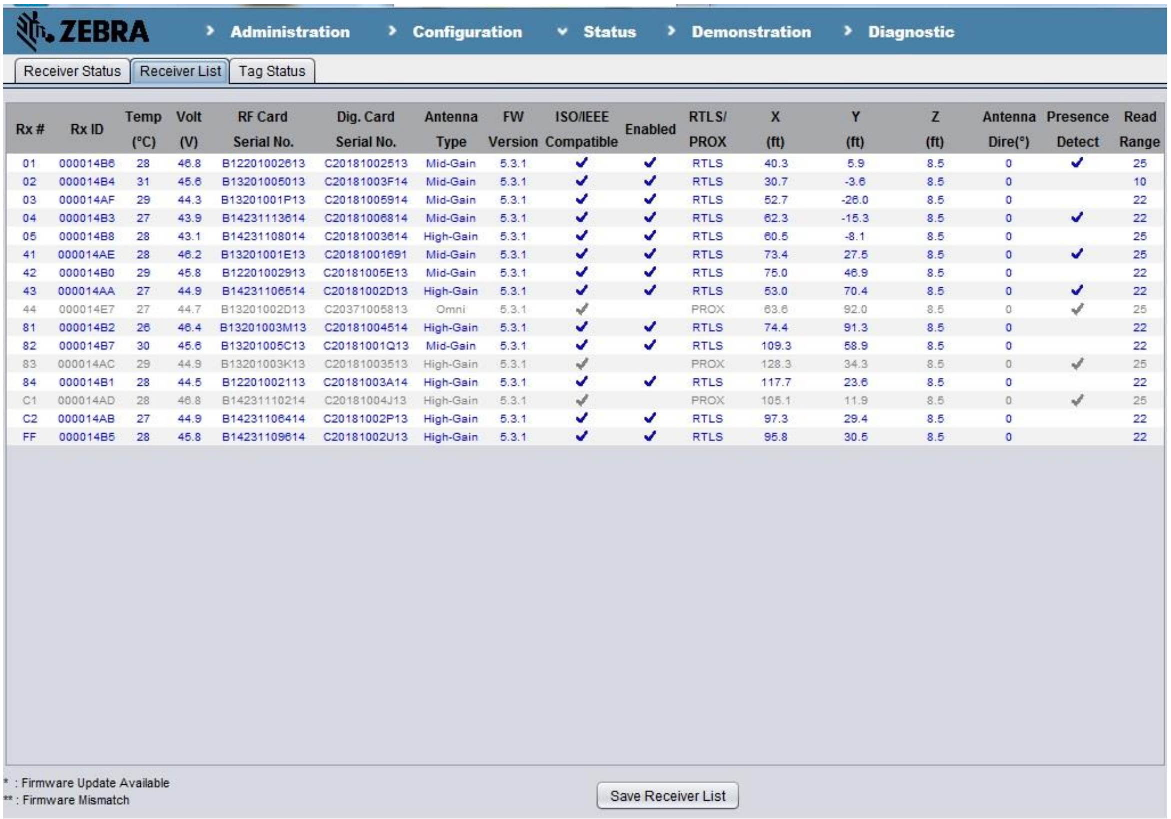
Viewing Receiver List

The Receiver **List** tab contains detail information, including receiver read range, temperature, hardware information for all Receivers detected by the hub.

To view Receiver status:

1 Start the **Hub Administration and Management** application, click **Status.**

2 On the **Receiver List** tab, examine the displayed information. This tab is automatically refreshed every 1 minute.



Rx #	Rx ID	Temp (°C)	Volt (V)	RF Card Serial No.	Dig. Card Serial No.	Antenna Type	FW Version	ISO/IEEE Compatible	Enabled	RTLS/ PROX	X (ft)	Y (ft)	Z (ft)	Antenna Dire(°)	Presence Detect	Read Range
01	000014B6	28	46.8	B12201002613	C20181002513	Mid-Gain	5.3.1	✓	✓	RTLS	40.3	5.9	8.5	0	✓	25
02	000014B4	31	45.6	B13201005013	C20181003F14	Mid-Gain	5.3.1	✓	✓	RTLS	30.7	-3.6	8.5	0		10
03	000014AF	29	44.3	B13201001P13	C20181005914	Mid-Gain	5.3.1	✓	✓	RTLS	52.7	-26.0	8.5	0		22
04	000014B3	27	43.9	B14231113614	C20181006814	Mid-Gain	5.3.1	✓	✓	RTLS	62.3	-15.3	8.5	0	✓	22
05	000014B8	28	43.1	B14231108014	C20181003614	High-Gain	5.3.1	✓	✓	RTLS	60.5	-8.1	8.5	0		25
41	000014AE	28	46.2	B13201001E13	C20181001691	Mid-Gain	5.3.1	✓	✓	RTLS	73.4	27.5	8.5	0	✓	25
42	000014B0	29	45.8	B12201002913	C20181005E13	Mid-Gain	5.3.1	✓	✓	RTLS	75.0	46.9	8.5	0		22
43	000014AA	27	44.9	B14231106514	C20181002D13	High-Gain	5.3.1	✓	✓	RTLS	53.0	70.4	8.5	0	✓	22
44	000014E7	27	44.7	B13201002D13	C20371005813	Omni	5.3.1	✓		PROX	63.6	92.0	8.5	0	✓	25
81	000014B2	26	46.4	B13201003M13	C20181004514	High-Gain	5.3.1	✓	✓	RTLS	74.4	91.3	8.5	0		22
82	000014B7	30	45.6	B13201005C13	C20181001Q13	Mid-Gain	5.3.1	✓	✓	RTLS	109.3	58.9	8.5	0		22
83	000014AC	29	44.9	B13201003K13	C20181003513	High-Gain	5.3.1	✓		PROX	128.3	34.3	8.5	0	✓	25
84	000014B1	28	44.5	B12201002113	C20181003A14	High-Gain	5.3.1	✓	✓	RTLS	117.7	23.6	8.5	0		22
C1	000014AD	28	46.8	B14231110214	C20181004J13	High-Gain	5.3.1	✓		PROX	105.1	11.9	8.5	0	✓	25
C2	000014AB	27	44.9	B14231106414	C20181002P13	High-Gain	5.3.1	✓	✓	RTLS	97.3	29.4	8.5	0		22
FF	000014B5	28	45.8	B14231109614	C20181002U13	High-Gain	5.3.1	✓	✓	RTLS	95.8	30.5	8.5	0		22

* : Firmware Update Available
** : Firmware Mismatch

This tab contains information for all receivers detected by the hub:

- **Rx #:** The receiver # of the receiver being configured. Otherwise, left blank.
- **Rx ID:** Corresponding Receiver ID for the detected receiver.
- **Temp:** The current temperature in Celsius at the receiver.
- **Volt:** The current input voltage at the receiver
- **RF Card Serial No:** Serial number for the Receiver RF board.
- **Dig Card Serial No:** Serial number for the Receiver Digital board.
- **Antenna Type**: Type of antenna installed on the receiver.
- **FW version**: Version number of the firmware currently running on the receiver.
- **ISO/IEEE Compatible**: Indicates if the receiver is compatible with receiving ISO/IEEE formatted tags.
- **Enabled:** Indicates if the receiver is enabled. When blank the receiver is disabled or not configured
- **RTLS/PROX:** Indicates if the receiver is configured to be a RTLS or Proximity receiver. When blank, the receiver is not configured.
- **Local:** Indicates whether the receiver is a local receiver, physically connected on this hub, or a remote receiver, physically connected on another hub, or remote hub.
- **X, Y, Z:** Location of the receiver being configured. Leave blank if the receiver is not configured.
- **Antenna Dire(°):** Direction of receiver antenna being configured. Leave blank if the

receiver is not configured.

- **Presence Detect:** Indicates a receiver (RTLS or Proximity) is configured to output presence data. This is left blank if the receiver is not configured.
- **Read Range:** Read range setting of a receiver (1 – 25 in coarse range control mode or 1 – 54 in fine range control mode). When blank, the receiver is not configured.
- **Remote Rx#:** Receiver number of the receiver as configured on the remote hub. This field is 00 if the receiver is local or not remote.
- **Remote Hub:** IP address of the remote hub that a remote receiver physically connected to. This field is all zeros if the receiver is local or not remote.

3 Click **Save Receiver List** to save all the receiver information to a text file for future reference.

Viewing Tag status

The **Tag Status** tab shows reference tag status and active tag detected.

To view Receiver status:

1 Start the **Hub Administration and Management** application, click **Status.**

2 On the **Tag Status** tab, examine the displayed information.

Component	Description
Active Tags	The tags currently detected by any Receiver in the system. The system removes a tag from this list if no Receiver has detected tag transmission for more than 60 seconds.
Reference Tags	The reference tag(s), with the battery condition and operation status. The reference tag status shows: • **Down** when a reference tag is not detected • **Suspended** when a reference is suspended from operation • **Present** when the battery level is in the recommended range The reference tag battery level shows: • **Low** when the tag's battery is low and needs to be changed • **Good** when the tag’s battery is good

14 Data Security

Data security in Dart hub is allowed via SSH tunneling.

In This Section

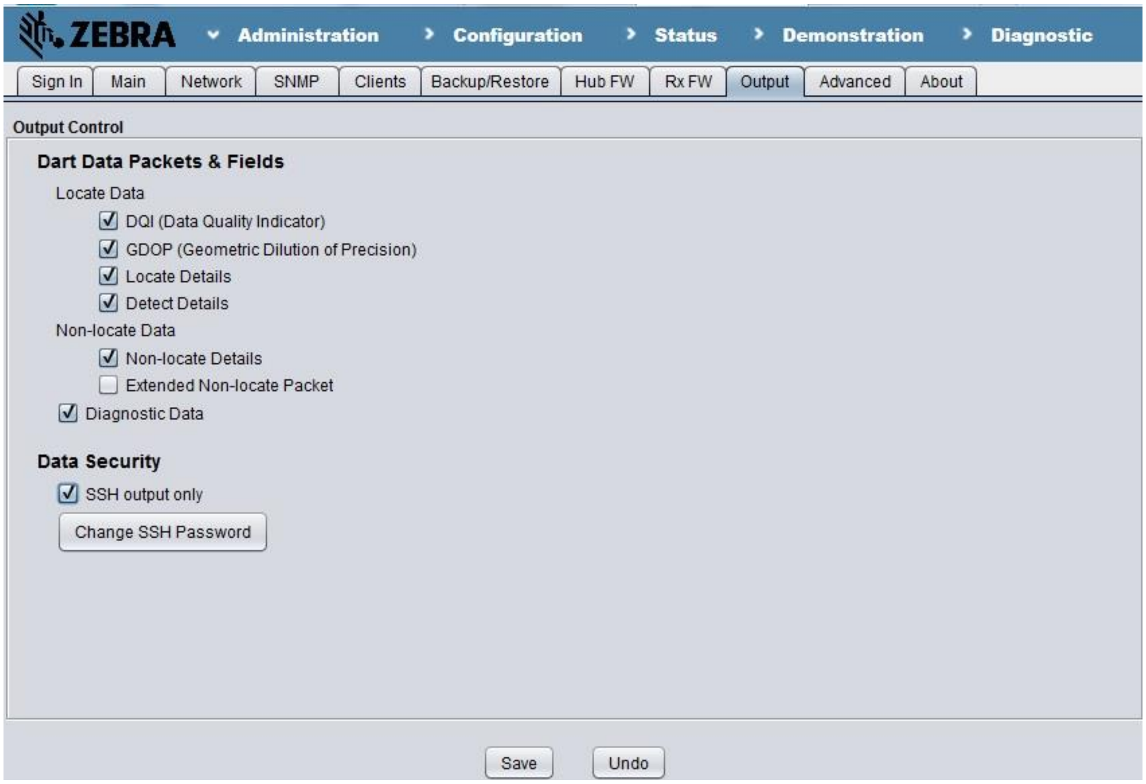
SSH user password

When manufactured, the SSH user is created in each Dart hub unit for creating SSH tunnel with Dart hub and receiving output data in an encrypted fashion. The user name is “`Dartssh`”, and its default password is “`Dartsshpwd1`”. The default password can be changed at user’s will.

To change SSH user password:

1 Start the **Hub Administration and Management** application, click **Administration.**

2 In the **Administration** view, select the **Output** tab.



Output Control

Dart Data Packets & Fields

Locate Data

- ☑ DQI (Data Quality Indicator)
- ☑ GDOP (Geometric Dilution of Precision)
- ☑ Locate Details
- ☑ Detect Details

Non-locate Data

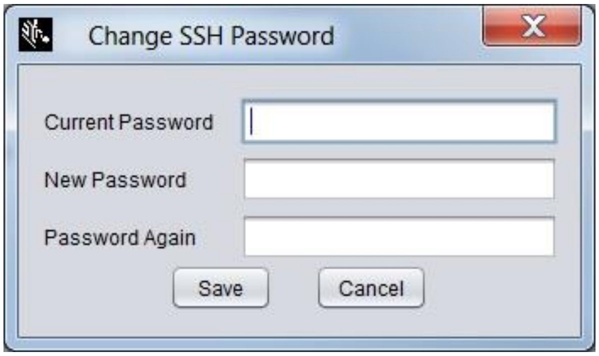
- ☑ Non-locate Details
- ☐ Extended Non-locate Packet

☑ Diagnostic Data

Data Security

☑ SSH output only

3 Check **Change Password**, **Change SSH Password** dialog appears.



4 Type the current SSH password and the new SSH password in input boxes, and click **Save** to accept it.

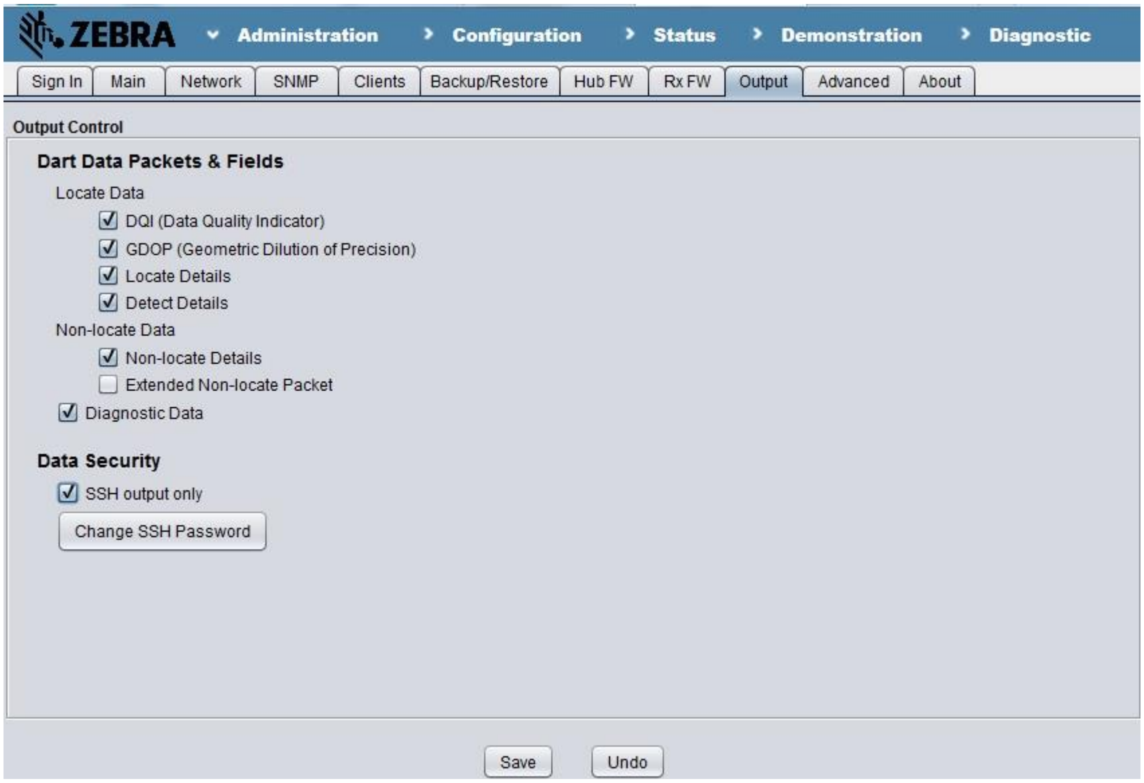
Non-secure data output

By default, Dart hub support output data in both secured and none-secured format**.** User can force data output only in secured fashion.

To disable non-secure data output:

1 Start the **Hub Administration and Management** application, click **Administration.**

2 In the **Administration** view, select the **Output** tab



Output Control

Dart Data Packets & Fields

Locate Data

☑ DQI (Data Quality Indicator)

☑ GDOP (Geometric Dilution of Precision)

☑ Locate Details

☑ Detect Details

Non-locate Data

☑ Non-locate Details

□ Extended Non-locate Packet

☑ Diagnostic Data

Data Security

☑ SSH output only

3 Check **SSH output only** box.

4 Click **Save** to make the change take effect.

Appendix A: Information Data (I-packets)

Dart Hub provides output data stream that are available on TCP port 5117. The data from the dart hub is coded in ASCII and sent over the LAN interface. To retrieve tag data from the hub, you need a client program using the TCP communication protocol and a connection to the output port. I packets are 'Information' packets that provide additional information about tag actions or sensor, like when tag is turned on/off, tag enters a WherePort field, sensor statistics etc.

I packet data is available on subscription only and client program needs to subscribe to it upon establishing a connection. I packet are provided in 2 different formats – Tag 'I' packet format that gives information about tag actions, and Receiver 'I' packet format, that gives information about receiver statistics. Receiver I packet provides statistics for each active receiver continuously on a 60 second interval.

Tag 'I' packet format:

Format of tag information packet is as follows:

```
   I,TagID,tagStatus,rate,battery,info,timestamp,evt_id,evt_msg

      TagID      - Tag ID

      tagStatus  - tag on/off state: 0: off; 1: on;  2: unknown

      rate       - tag blink rate in Hz

      battery    - tag battery report

      info       - event specific information

      timestamp  - timestamp of reporting time

      evt_id     - event type ID

      evt_msg    - event message
```

```
Example:

I,00200E8F,1,2.00,12,0,1435161191.102,3,'DartWand changed tag blink rate'
```

Tag 'I' packet table:

Evt_id	Evt_msg	Description	Info
0	Tag Resets	Tag Reset (due to low battery?)	Extended information from the tag
1	Dart Wand turned tag on	Dart wand turned on a tag which was previously off	0
2	Dart Wand turned tag off	Dart wand turned a tag off which was previously on	0
3	Dart Wand changed tag blink rate	Dart wand changed the blink rate of the tag	0
4	Whereport turned tag on	Tag, previously off, was turned on upon entering a (configured) WherePort field.	Whereport ID
5	Whereport turned tag off	Tag, previously on, was turned off upon entering a (configured) WherePort field.	Whereport ID
6	Accelerometer changed tag blink rate	Motion sensor within the tag caused the tag to change its blink rate.	Rate number (0/1/2)
7	Whereport changed tag blink rate	Configured Whereport changed the blink rate of the tag	Whereport ID
8	Tag passed through whereport field	Tag passed through the (configured) WherePort field, but no action was performed by the WherePort.	Whereport ID
9	Tag encountered an unknown whereport	Tag encountered a whereport not configured in the hub.	Whereport ID
11	Tag experienced momentary movement	Motion sensor within the tag detected a momentary movement	Event Count
12	Tag rotation started	Motion sensor within the tag detected the start of rotation	Event Count
13	Tag rotation stopped	Motion sensor within the tag detected the end of rotation	Event Count

Receiver 'I' packet format:

Format of receiver information packet is as follows:

```
I,Rx number,Overflow count, CRC error count,Bad header count,Bad packet format
count,timestamp,evt_id,evt_msg

    Rx number – active receiver number

    Overflow count – FIFO overflow count

    CRC error count- Number of packet CRC errors

    Bad header count – Bad message header count

    Bad packet format count – Number of packet format errors

    timestamp  - timestamp of reporting time

    evt_id     - event type ID

    evt_msg    - event message
```

```
Example:
```

I,82,0,0,0,0,1446750504.003,10,'Receiver communication statistics'

Receiver 'I' Packet Table:

Evt_id	Evt_msg	Description
10	Receiver communication statistics	Receiver statistics for each active sensor is sent out every 60 seconds.

Appendix B: Diagnostic Output Data (D-packets)

This section contains descriptions for all D-packets that Dart UWB RTLS may output.

D-packets are sent to the output stream only when enabled on the **Output Control** tab of the **Hub Configuration** form (See ***Configuring output control*** (on page 43)). These messages are either error or warning messages that are useful both during initial installation and for continuous monitoring of the Dart RTLS system. For critical system errors, the corresponding D-packets will be continuously sent until the error condition has been cleared. For non-critical error or events, the corresponding D-packets will be sent only once each time there is an event/error condition.

D-packets present in the Dart formatted output data stream (port 5117). D packets in the Dart output stream follow a common format as follows:

D,<ID>,<X>,<Y>,<Z>,<battery>,<timestamp>,<DpacketID>,'event text string'<LF>

D-packets are sent during firmware initialization, after a firmware restart and during normal operation.

During normal operation, D-packet outputs are event driven, and sent each time there is a state change in the status of either a reference tag or Receiver. Errors sent during initialization will typically indicate either hardware or software setup errors.

Initialization Actions	• Verifies Receivers are configured & available • Verifies reference tag(s) are configured & available • Verifies virtual groups configured

Initialization D-packets	• No Receiver detected • No Receiver enabled • No Receiver activated • No reference tag enabled • No virtual group enabled • Enabled Receiver detected • Enabled Receiver not detected • Unknown Receiver detected • Receiver 00 detected • Receiver has detected a reference tag • Reference tag not found • Receiver firmware upgrade available • Receiver firmware mismatch • Reference tag suspended • Reference tag suspension fail • Reference pair broken • Restart start • Restart end • Hub Failure • Health state change • USB Rx Failure • Health tag not found • Health tag detected • NTP sync failed • NTP sync succeeded • Remote Hub connection failed • Remote Hub connection succeeded • Hub sync 100M clock error • Hub sync 100M clock good
Operation Actions	• Polls tag data from all active Receivers • Verifies reference tags detected by all active Receivers • Computes tag positions

Operation D-packets	• Active Receiver communication lost • Active Receiver communication OK • Reference tag detected • Reference tag lost • Reference tag battery low • Reference tag battery OK • Receiver does not see reference tag • Receiver has detected the reference tag • Active Receiver loss of referencing • Server is alive • Hub Failure • Health state change • CPU temperature too high • USB Rx Failure • Health tag failure • Health tag battery low • Health tag battery OK • Health tag not found • Health tag detected • NTP sync failed • NTP sync succeeded • Remote Hub connection failed • Remote Hub connection succeeded • Hub Sync 100M clock error • Hub Sync 100M clock good

D-packets possible during initialization and installation

No Receiver enabled	• **Description:** Configuration setup warning; no Receivers have been defined in the Hub. • **Recommended Action:** Enable one or more Receivers using the Hub’s Configuration menu. • **Message Type:** This error packet will be sent continuously until the error condition is cleared. • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,‘Error: no receiver enabled’
No reference tag enabled	• **Description:** Configuration setup warning; no reference tags have been defined in the Hub. • **Recommended Action:** Enable one or more reference tags using the Hub Configuration menu. • **Message Type:** This warning packet will be sent once after a Hub firmware restart. • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,‘Error: no reference tag enabled’
No virtual group enabled	• **Description:** Configuration setup warning; no virtual groups have been enabled in the Hub. • **Recommended Action:** Enable one or more virtual groups using the Hub’s Configuration menu. • **Message Type:** This warning packet will be sent once after a Hub firmware restart. • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,‘Error: no virtual group enabled’

No Receiver detected	• **Description:** No Receivers have been detected by the Hub. • **Recommended Action:** Verify connections and power from the Hub to the Receiver (s). • **Message Type:** This error packet will be sent continuously until the error condition is cleared. • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,'Error: no receiver detected'
No Receiver activated	• **Description:** A Receiver or Receivers have been detected, but none are enabled to send messages to the Hub. • **Recommended Action:** A Receiver may be detected, but not enabled. Activate the Receiver through the Hub's Configuration menu. • **Message Type:** This error packet will be sent continuously until the error condition is cleared. • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,'Error: no receiver activated'
Enabled Receiver not detected	• **Description:** An individual Receiver with Receiver # <Rx#>, which is configured and enabled at location (x, y, z), has not been detected or has never communicated with the Hub since firmware restart. • **Recommended Action:** User should verify connections and power from the Hub to the Receiver (s). • **Message Type:** The warning packet will be sent only once after a Hub firmware restart. • **Message Format:** **Dart:** D,Rx#,x,y,z,0,timestamp,DpacketID,'Error: Enabled receiver not detected'
Enabled Receiver detected	• **Description:** A Receiver with a Receiver# <Rx#>, which is configured and enabled at location (x,y,z), has been detected for the first time since a Hub firmware restart. • **Recommended Action:** None. • **Message Type:** This D packet will be sent once for each active Receiver after a Hub firmware restart. • **Message Format:** **Dart:** D,Rx#,x,y,z,0,timestamp,DpacketID,'Enabled receiver detected'
Unknown Receiver detected	• **Description:** A Receiver with Receiver ID <RxID>, which is not configured in the Hub's Configuration menu, has been detected after the Hub firmware restart. • **Recommended Action:** Verify that all expected receivers configured in the Hub's Configuration menu are detected in the Status and Control menu. It is possible that you will either need to activate the unknown Receiver through the Hub's Configuration menu or change the rotary settings for the RX ID to the expected hexadecimal value. • **Message Type:** This warning packet will be sent only once upon the detection after a Hub firmware restart. • **Message Format:** **Dart:** D,RxID,0,0,0,0,timestamp,DpacketID,'Warning: unknown receiver detected'.

Receiver 00 detected	• **Description:** Old Receiver (with 1 byte serial number) shipped with ’00’ ID has not been configured to a valid serial number. • **Recommended Action:** Configure the serial number on the receiver to something other than ‘00’ (configuration has to be manually done on the side of the receiver). • **Message Type:** This warning packet will be sent only once upon the detection after a Hub firmware restart. • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,‘Warning: receiver 00 detected’
Reference tag not found	• **Description:** A reference tag with tag ID <refTagID>, configured to be at location (x,y,z), has not been detected since firmware restart. The <battery> represents the tag battery level at the last detection time, and <timestamp> is the UNIX time (that is the number of elapsed seconds since January 1, 1970, UTC) when this event is reported. • **Recommended Action:** Verify the reference tag is present and not damaged. • **Message Type:** This error packet will be sent continuously until the error condition is cleared. • **Message Format:** **Dart –** D,refTagID,x,y,z,battery,timestamp,DpacketID,‘Error: reference tag not found’
Receiver has detected a reference tag	• **Description:** An active Receiver with Receiver #ID <Rx#>, which is configured at location (x, y, z), has seen one of its associated reference tags after a Hub firmware restart. • **Recommended Action:** None. • **Message Type:** This information packet is sent only once when the Receiver detects the reference tag for the first time since Hub firmware restart or it had been reported as the Receiver has not seen the reference tag. • **Message Format:** **Dart:** D,Rx#,x,y,z,refTagID,timestamp,DpacketID,‘Receiver has detected the reference tag <refTagID> ‘
Receiver firmware upgrade available	• **Description:** One or more detected Receivers have old firmware, and new firmware is available for upgrade. • **Recommended Action:** Visit **Update** Receiver tab in the **Administration** page to identify Receiver (s) with old firmware, and upgrade them with the latest firmware uploaded to the hub. • **Message Type:** This warning packet will be sent only once after a hub firmware restart. • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,‘Warning: Receiver FW upgrade available ‘
Receiver firmware mis-match	• **Description:** One or more detected Receivers have firmware newer than the one uploaded to the hub. • **Recommended Action:** Contact Customer Support to get the latest Receiver firmware, and upgrade it to all Receiver (s). • **Message Type:** This warning packet will be sent only once after a hub firmware restart. • **Message Format:** **Dart:** D,0,0,0,0,0,,timestamp,DpacketID,‘Warning: Receiver FW mis-match ‘

Reference tag suspended	• **Description:** All enabled reference tags are suspended as required by configuration. • **Recommended Action:** None • **Message Type:** This packet will be sent only once after a hub firmware restart • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,'reference tag suspended'
Reference tag suspension fail	• **Description:** Required reference suspension failed because a consistent and complete referencing cross the RTLS system cannot be obtained within 30 seconds after hub firmware restart. • **Recommended Action:** Check if each receiver has line of sight of associated reference tag(s). Check correctness of receivers' location and reference tags' location. • **Message Type:** This warning packet will be sent continuously until the error condition is cleared • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,'Error: reference tag suspension fail'
Reference pair broken	• **Description:** When reference tag suspension is required, and two active receivers (Rx#1 and Rx#2) should establish consistent timing reference based on configuration, if the referencing cannot achieve in the 30 seconds after hub firmware restart, this D-packet message will be sent out. • **Recommended Action:** Check if both receiver has line of sight of associated reference tag(s). Check correctness of receivers' location and reference tags' location. • **Message Type:** This warning packet will be sent only once after a hub firmware restart • **Message Format**: **Dart**: D,Rx#1,0,0,0,Rx#2,timestamp,DpacketID,'Error: reference pair broken (Rx#1 Rx#2)'
Restart start	• **Description:** Hub firmware restart starts. • **Recommended Action:** None. • **Message Type:** This packet will be sent only once after hub firmware restart • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,'Restart start'
Restart end	• **Description:** Hub firmware restart completes. • **Recommended Action:** None. • **Message Type:** This packet will be sent only once after hub firmware restart • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,'Restart end'
Hub Failure	• **Description:** This D-packet message is sent when the system auto recovers from an unexpected system fault. • **Recommended Action:** None. • **Message Type:** Sent every minute until system reboot is performed. • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,'Error:Kernel Reboot.'

Health State Change	• **Description:** This D-packet message is sent when there is a change in system health state. • **Recommended Action:** None. • **Message Type:** The event packet is sent only once whenever a change in system health state is detected. • **Message Format:** **Dart:** D, Current_Health_State, Latched_Health_State, Outstanding_Error_Types, Outstanding_Warning_Types, 0, timestamp, DpacketID,'Health State Change.'
USB Rx Failure	• **Description:** This D-packet message is sent when there are consecutive USB receive failures. • **Recommended Action:** None. • **Message Type:** Sent every instance where 5 or more consecutive receive failures are detected. • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,'Error:USB receiving failure.' •
Health tag not found	• **Description:** A health tag with tag ID <hthTagID>, configured to be at location (x,y,z), has lost signal for more than 20 seconds. The <battery> represents the tag battery level at the last detection time, and <timestamp> is the UNIX time (i.e. the number of elapsed seconds since January 1, 1970, UTC), at which the health tag signal was last detected. • **Recommended Action:** Verify the health tag is present and not damaged. • **Message Type:** This warning packet will be sent only once when the health tag has not been detected for 20 seconds • **Message Format:** **Dart:** D,hthTagID,x,y,z,battery,timestamp,DpacketID,'Error: Health tag not found'
Health tag detected	• **Description:** A health tag with tag ID <hthTagID>, configured to be at location(x,y,z), is detected with a tag battery level of <battery> at UNIX time of <timestamp>. • **Recommended Action:** None. • **Message Type:** This event packet will be sent only once when the health tag is detected for the first time since firmware restart or it had been reported as lost. • **Message Format:** **Dart:** D,hthTagID,x,y,z,battery,timestamp,DpacketID,'Health tag detected'
NTP sync succeeded	• **Description:** NTP synchronization succeeded at UNIX time of <timestamp>. • **Recommended Action:** None. • **Message Type:** This event packet will be sent only once when the NTP synchronization succeeds. • **Message Format:** • **Dart:** D,0,0,0,0,0,timestamp,DpacketID,'NTP synchronization succeeded'
NTP sync failed	• **Description:** NTP synchronization failed at UNIX time of <timestamp>. • **Recommended Action:** None. • **Message Type:** This event packet will be sent after every retry to attempt to sync with the NTP server. • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,'Error: NTP synchronization failed'

Remote Hub Connection failed	• **Description:** An attempt to connect to a remote hub failed at UNIX time of <timestamp>. • **Recommended Action:** Check network cable and whether remote hub is functioning. • **Message Type:** This event packet will be sent after every retry to connect with the remote hub and will persist until a connection can be established. • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,‘Error: Remote hub connection failed’
Remote Hub Connections succeeded	• **Description:** An attempt to connect to a remote hub succeeded at UNIX time of <timestamp>. • **Recommended Action:** None. • **Message Type:** This event packet will be sent once when an attempt to connect with the remote hub succeeds. • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,‘ Remote hub connection succeeded’
Hub Sync 100M Clock error	• **Description:** Clock sync failed between hubs that share receivers, at UNIX time of <timestamp>. • **Recommended Action:** Check the RJ45 cable between hubs are connected in a daisy chain. There can by only one master hub supplying the clock in a chain of connected hubs. • **Message Type:** This event packet will be sent every minute until clock sync is established between hubs. • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,‘ Error: Hub sync 100M clock error’
Hub Sync 100M clock good	• **Description:** Clock sync OK between hubs that share receivers, at UNIX time of <timestamp>. • **Recommended Action:** None. • **Message Type:** This event packet will be sent once when clock sync is established between hubs. • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,‘ Hub sync 100M clock good’

If a new Receiver is detected, the firmware automatically restarts to enable this Receiver for all computations.

D-packets possible during operation

Reference tag lost	• **Description:** A reference tag with tag ID <refTagID>, configured to be at location (x,y,z), has lost signal for more than 20 seconds. The <battery> represents the tag battery level at the last detection time, and <timestamp> is the UNIX time (i.e. the number of elapsed seconds since January 1, 1970, UTC), at which the reference tag signal was last detected. • **Recommended Action:** Verify the reference tag is present and not damaged. • **Message Type:** This warning packet will be sent only once when the reference tag has not been detected for 20 seconds • **Message Format:** **Dart:** D,refTagID,x,y,z,battery,timestamp,DpacketID,‘Error: reference tag lost’

Reference tag detected	• **Description:** A reference tag with tag ID <refTagID>, configured to be at location(x,y,z), is detected with a tag battery level of <battery> at UNIX time of <timestamp>. • **Recommended Action:** None. • **Message Type:** This event packet will be sent only once when the reference tag is detected for the first time since firmware restart or it had been reported as lost. • **Message Format:** **Dart:** D,refTagID,x,y,z,battery,timestamp,DpacketID,'Reference tag detected'
Reference tag battery low	• **Description:** This D-packet message is sent approximately every minute on each reference tag whose battery is low. After receiving 60 consecutive tag reports from a reference tag with battery level equal or less than '9', the Dart RTLS Hub puts the reference tag into battery condition. This message will be cleared once the battery status is at a value above 9. • **Recommended Action:** Replace reference tag. • **Message Type:** Sent every minute. • **Message Format:** **Dart:** D,refTagID,x,y,z,battery,timestamp,DpacketID,'Warning: Reference tag battery low'
Reference tag battery OK	• **Description:** A reference tag configured at location (x, y, z) recovered from battery low condition. When a reference gets into battery low condition, once its battery status is at a value above the threshold, it exits from battery low condition and send this D-packet once • **Recommended Action:** None. • **Message Type:** This event packet will be sent only once after the reference tag exits from battery low condition. • **Message Format:** **Dart:** D,refTagID,x,y,z,battery,timestamp,DpacketID,'Reference tag battery OK'
Receiver does not see reference tag	• **Description:** An active Receiver with Receiver # <Rx#>, which is configured at location (x, y, z), has not seen one of its associated reference tags for at least 20 seconds • **Recommended Action:** Verify that Receiver with Receiver # <Rx#> has power and is within range of the reference tag. • **Message Type:** This warning message will be sent only when the Receiver does not detect the reference tag for more than 20 seconds. • **Message Format:** **Dart:** D,Rx#,x,y,z,refTagID,timestamp,DpacketID,'Warning: receiver does not see the reference tag <refTagID>'
Receiver has detected a reference tag	• **Description:** An active Receiver with Receiver # <Rx#>, which is configured at location (x, y, z), has seen one of its associated reference tags after a Hub firmware restart. • **Recommended Action:** None. • **Message Type:** This information packet is sent only once when the Receiver detects the reference tag for the first time since Hub firmware restart or it had been reported as the Receiver has not seen the reference tag. • **Message Format:** **Dart:** D,Rx#,x,y,z,refTagID,timestamp,DpacketID,'Receiver has detected the reference tag <refTagID>'

Active Receiver communication lost	• **Description:** An active Receiver with a Receiver # <Rx#>, which is configured to be at location (x, y, z), has lost normal communication to the Hub. The <battery> field is always 0, and <timestamp> represents the last time (in UTC format) when the Hub is still able to communicate with the Receiver. • **Recommended Action:** Verify the Receiver is present, powered on, and not damaged. • **Message Type:** The event packet will be sent only once after the Hub lost the communication with the Receiver. • **Message Format:** **Dart:** D,Rx#,x,y,z,0,timestamp,DpacketID,'Error: active Receiver communication lost'
Active Receiver communication OK	• **Description:** An active Receiver with a Receiver # <Rx#>, which is configured to be at location(x,y,z), has re-established a normal communication to the Hub after previous loss-of-communication. The <battery> field is always 0, and <timestamp> represents the UTC time that the Hub starts to communicate with the Receiver again. • **Recommended Action:** None. • **Message Type:** The event packet will be sent only once when the Hub re-gains communication with the Receiver. • **Message Format:** **Dart:** D,Rx#,x,y,z,0,timestamp,DpacketID,'Active Receiver communication OK'
Active Receiver loss of referencing	• **Description:** An active Receiver with a Receiver # <Rx#>, which is configured to be at location(x,y,z), has lost referencing after it recovers from loss- of-communication because all reference tags are suspended The <battery> field is always 0, and <timestamp> represents the UTC time that the receiver recovers from loss-of-communication. • **Recommended Action:** Restart the hub firmware. • **Message Type:** Sent every minute. • **Message Format:** **Dart:** D,Rx#,x,y,z,0,timestamp,DpacketID,'Error: active Receiver loss of referencing'
Server is alive	• **Description:** This D-packet message is sent approximately every minute to indicate the Hub and socket connection is operational. The Dart format of Dart RTLS server alive diagnostic message now also includes system health status and total number of currently established data clients (Dart, ISO or Z-SLMF). • **Recommended Action:** None. • **Message Type:** Sent every minute. • **Message Format:** **Dart:** D,Current_Health_State,Latched_Health_State,Outstanding_Error_Types,Outstanding_Warning_Types,Data_Client_Count,timestamp,DpacketID,'Server is alive.'
Hub Failure	• **Description:** This D-packet message is sent when the system auto recovers from an unexpected system fault. • **Recommended Action:** None. • **Message Type:** Sent every minute until system reboot is performed. • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,'Error:Kernel Reboot.'

Health State Change	• **Description:** This D-packet message is sent when there is a change in system health state. • **Recommended Action:** None. • **Message Type:** The event packet is sent only once whenever a change in system health state is detected. • **Message Format:** **Dart:** D, Current_Health_State, Latched_Health_State, Outstanding_Error_Types, Outstanding_Warning_Types, 0, timestamp, DpacketID,'Health State Change.'
CPU temperature too high	• **Description:** This D-packet message is generated if the CPU temperature of UWH-1200 hub is too high (above 85C). • **Recommended Action:** Inspect the environment to see what is causing the temperature to spike. • **Message Type:** The event packet is sent every minute until the temperature drops back down below 85C. • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,'Error: CPU temperature too high'
USB Rx Failure	• **Description:** This D-packet message is sent when there are consecutive USB receive failures. • **Recommended Action:** None. • **Message Type:** Sent every instance where 5 or more consecutive receive failures are detected. • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,'Error:USB receiving failure.' •
Health Tag Failure	• **Description:** A health tag with tag ID <hthTagID>, configured to be at location(x,y,z), has a locate percentage or error radius value over the threshold specified. • **Recommended Action:** None. • **Message Type:** This event packet is persisted until the locate percentage and error radius values fall back within threholds specified for the measurement period specified. • **Message Format:** **Dart:** D,hthTagID,x,y,z,battery,timestamp,DpacketID,'Error:health tag failure(Locate percentage Error radius)'
Health tag battery low	• **Description:** This D-packet message is sent approximately every minute on each health tag whose battery is low. After receiving 60 consecutive tag reports from a health tag with battery level as low, the Dart RTLS Hub puts the health tag into battery low condition. This message will be cleared once the battery status is normal again. • **Recommended Action:** Replace health tag. • **Message Type:** Sent every minute. • **Message Format:** **Dart:** D,hthTagID,x,y,z,battery,timestamp,DpacketID,'Warning: Health tag battery low'

Health tag battery OK	• **Description:** A health tag configured at location (x, y, z) recovered from battery low condition. When a health tag gets into battery low condition, once its battery status is at a value above the threshold, it exits from battery low condition and send this D-packet once • **Recommended Action:** None. • **Message Type:** This event packet will be sent only once after the health tag exits from battery low condition. • **Message Format:** **Dart:** D,hthTagID,x,y,z,battery,timestamp,DpacketID,‘Health tag battery OK’
Health tag not found	• **Description:** A health tag with tag ID <hthTagID>, configured to be at location (x,y,z), has lost signal for more than 20 seconds. The <battery> represents the tag battery level at the last detection time, and <timestamp> is the UNIX time (i.e. the number of elapsed seconds since January 1, 1970, UTC), at which the health tag signal was last detected. • **Recommended Action:** Verify the health tag is present and not damaged**.** • **Message Type:** This warning packet will be sent only once when the health tag has not been detected for 20 seconds • **Message Format:** **Dart:** D,hthTagID,x,y,z,battery,timestamp,DpacketID,‘Error: Health tag not found’
Health tag detected	• **Description:** A health tag with tag ID <hthTagID>, configured to be at location(x,y,z), is detected with a tag battery level of <battery> at UNIX time of <timestamp>. • **Recommended Action:** None. • **Message Type:** This event packet will be sent only once when the health tag is detected for the first time since firmware restart or it had been reported as lost. • **Message Format:** **Dart:** D,hthTagID,x,y,z,battery,timestamp,DpacketID,‘Health tag detected’
NTP sync succeeded	• **Description:** NTP synchronization succeeded at UNIX time of <timestamp>. • **Recommended Action:** None. • **Message Type:** This event packet will be sent only once when the NTP synchronization succeeds. • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,‘NTP synchronization succeeded’
NTP sync failed	• **Description:** NTP synchronization failed at UNIX time of <timestamp>. • **Recommended Action:** None. • **Message Type:** This event packet will be sent after every retry to attempt to sync with the NTP server. • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,‘Error: NTP synchronization failed’
Remote Hub Connection failed	• **Description:** An attempt to connect to a remote hub failed at UNIX time of <timestamp>. • **Recommended Action:** Check network cable and whether remote hub is functioning. • **Message Type:** This event packet will be sent after every retry to connect with the remote hub and will persist until a connection can be established. • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,‘Error: Remote hub connection failed’

Remote Hub Connections succeeded	• **Description:** An attempt to connect to a remote hub succeeded at UNIX time of <timestamp>. • **Recommended Action:** None. • **Message Type:** This event packet will be sent once when an attempt to connect with the remote hub succeeds. • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,‘ Remote hub connection succeeded’
Hub Sync 100M Clock error	• **Description:** Clock sync failed between hubs that share receivers, at UNIX time of <timestamp>. • **Recommended Action:** Check the RJ45 cable between hubs are connected in a daisy chain. There can by only one master hub supplying the clock in a chain of connected hubs. • **Message Type:** This event packet will be sent every minute until clock sync is established between hubs. • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,‘ Error: Hub sync 100M clock error’
Hub Sync 100M clock good	• **Description:** Clock sync OK between hubs that share receivers, at UNIX time of <timestamp>. • **Recommended Action:** None. • **Message Type:** This event packet will be sent once when clock sync is established between hubs. • **Message Format:** **Dart:** D,0,0,0,0,0,timestamp,DpacketID,‘ Hub sync 100M clock good’

D-packet event messages

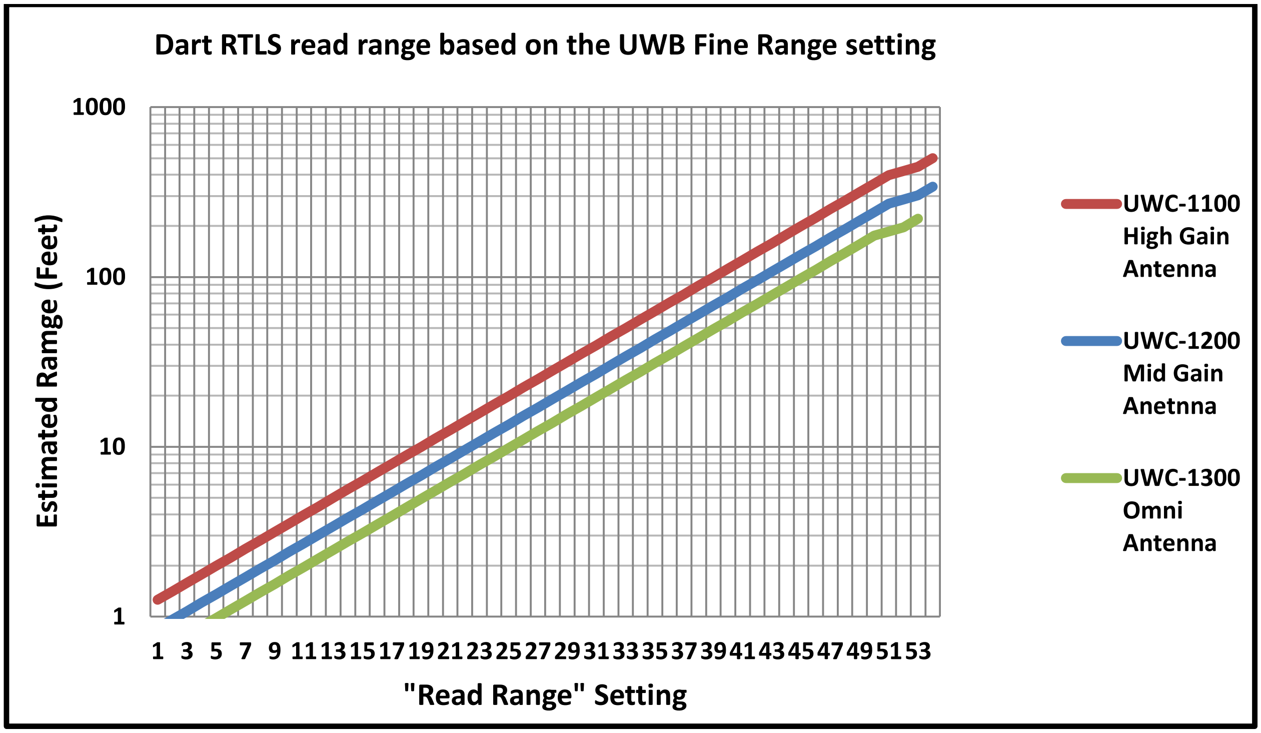
D-Packet	D-packet ID	Message Type	Continuous Message?
No Receiver enabled	-10	Error	✓
No reference tag enabled	-20	Error	
Reference tag battery low	-22	Warning	✓
Reference tag battery OK	22	Status	
No virtual group enabled	-30	Error	
No Receiver detected	-11	Error	✓
No Receiver activated	-12	Error	✓
Enabled Receiver detected	13	Status	
Enabled Receiver not detected	-13	Error	
Unknown Receiver detected	-14	Warning	
Unknown Receiver removed	14	Status	
Receiver 00 detected	-15	Warning	
Receiver does not see the reference tag	-16	Warning	
Receiver has detected reference tag	16	Status	
Reference tag detected	21	Status	
Reference tag lost	-21	Error	
Reference tag not found	-23	Error	✓
Active Receiver communication lost	-17	Error	

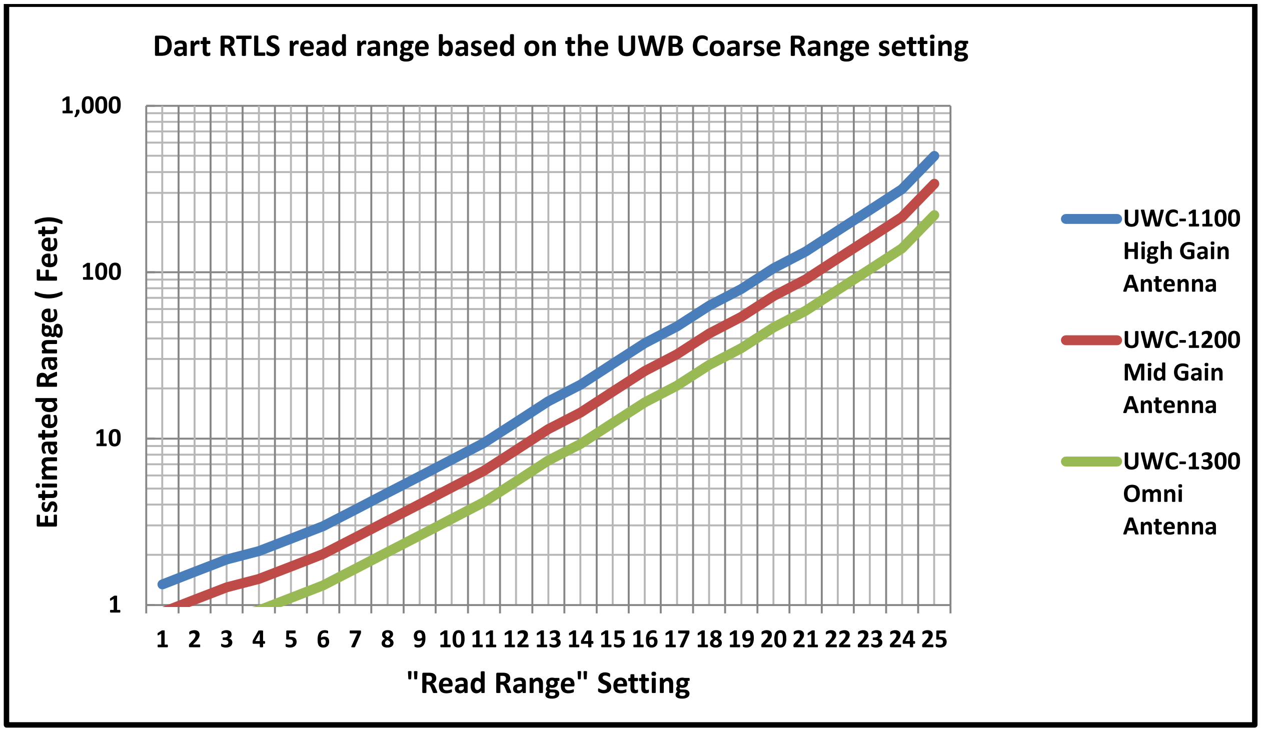
D-Packet	D-packet ID	Message Type	Continuous Message?
Active Receiver communication OK	17	Status	
Receiver firmware upgrade available	-18	Warning	
Receiver firmware mis-match	-19	Warning	
Server is alive	1	Status	✓
Reference pair broken	-24	Error	
Reference tag suspended	25	Status	
Reference tag suspension fail	-25	Error	
Receiver loss of referencing	-35	Error	✓
Restart start	2	Status	
Restart end	3	Status	
Health state change	4	Status	
CPU temperature too high	-5	Error	✓
Hub Failure	-6	Error	✓
USB Rx Failure	-9	Error	
Health tag failure	-26	Error	✓
Health tag battery low	-27	Warning	✓
Health tag battery OK	27	Status	
Health tag not found	-28	Error	
Health tag detected	28	Status	
NTP sync failed	-42	Error	
NTP sync succeed	42	Status	
Remote hub connection failed	-43	Error	✓
Remote hub connection succeed	43	Status	
Hub sync 100M clock error	-44	Error	✓
Hub sync 100M clock good	44	Status	

Appendix C: Receiver read range settings

The Dart hub provides two control modes for Receiver read range: coarse mode and fine mode. Coarse control mode is the default mode, which allows read range setting of a Receiver to be set from 1 to 25, where 1 is the smallest read range setting and 25 is the largest read range setting. In fine control mode, read range settings vary from 1 to 54, where 1 is the least sensitive (shortest read range) and 54 is the most sensitive (longest read range) setting.

The following figures, one for coarse control mode, one for fine control mode, provide guidelines on approximating read range settings based on Receiver antenna type in a line of sight environment. This table is intended to be used a guideline. Actual ranges will vary based on the presence of RF obstructions and adverse reflections. Range measurements are shown for line of sight conditions. Ranges are typically decreased as the result of obstructions, whereas adverse reflections can create areas of cancellation or enhancement of the signals which can be unpredictable and are often non-intuitive. For these reasons, it is recommended to verify read ranges experimentally for each application.

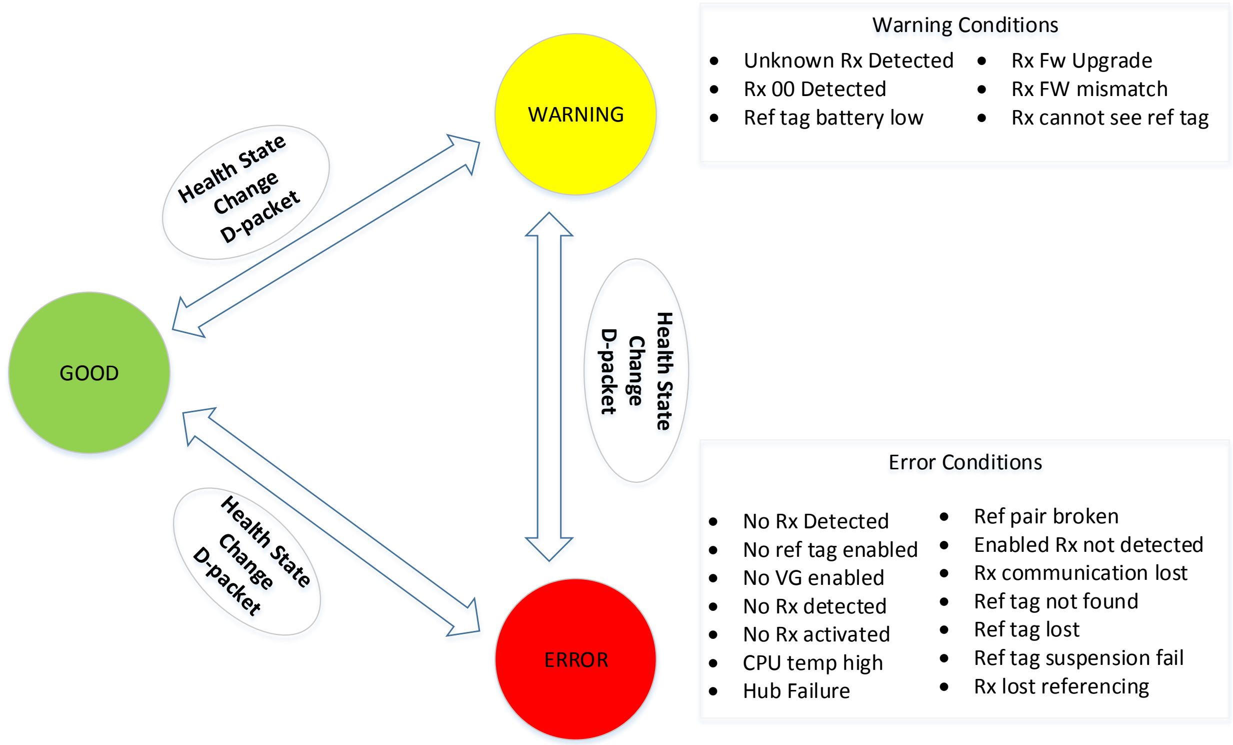



Dart RTLS read range based on the UWB Coarse Range setting
Estimated Range (Feet)
1,000
100
10
1
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
"Read Range" Setting
UWC-1100 High Gain Antenna
UWC-1200 Mid Gain Antenna
UWC-1300 Omni Antenna

Appendix D: Hub Health Monitoring

This section contains details of the health monitor module inside the Dart RTLS hub. Health monitor is a new feature inside hub RTLS firmware that latches the health of the Dart RTLS system and sends out D packets when there is a change in the health status.

Health monitor represents Dart RTLS system in three health states: good(green), warning(yellow) and error(Red) and corresponding state machine is as follows:


WARNING
GOOD
ERROR
Health State Change D-packet
Health State Change D-packet
Health State Change D-packet

Warning Conditions

- Unknown Rx Detected
- Rx 00 Detected
- Ref tag battery low
- Rx Fw Upgrade
- Rx FW mismatch
- Rx cannot see ref tag

Error Conditions

- No Rx Detected
- No ref tag enabled
- No VG enabled
- No Rx detected
- No Rx activated
- CPU temp high
- Hub Failure
- Ref pair broken
- Enabled Rx not detected
- Rx communication lost
- Ref tag not found
- Ref tag lost
- Ref tag suspension fail
- Rx lost referencing

Dart RTLS System Health Monitor States

Health Status Parameters

Health monitoring uses a set of parameters to describe the health status of Dart RTLS system at any time, and the set of parameters are:

Current_Health_State - current health state of a Dart RTLS system. It has three values: 0 (green), 1 (yellow) and 2 (red).

Latched_Health_State - the worst health state a Dart RTLS system has experienced since firmware restart. It also has three values: 0 (green), 1 (yellow) and 2 (red).

Outstanding_Error_Types – types of current outstanding errors at a Dart RTLS system. It is a bit-wise value with each bit defined as follows:

Bit number	Error Type
0	Configuration Error
1	No Rx detected
2	No Rx activated
3	Enabled Rx not detected
4	Reference tag not found
5	Reference suspension failed
6	CPU temperature high
7	Hub Failure
8	Health tag not found
9	USB Rx failure
10	NTP Sync failure
11	Remote Hub Connection fail
12	Hub Sync clock error
10-15	Reserved
16	Rx communication loss
17	Reference tag loss
18	Rx referencing loss
19	Reference pair broken
20	Health tag failure

Outstanding_Warning_Types – types of current outstanding warnings at a Dart RTLS system. It is a bit-wise value with each bit defined as follows:

Bit number	Warning Type
0	Unknown Rx detected
1	Rx 00 detected
2	Rx firmware upgrade
3	Rx firmware mismatch
4	Hub FPGA FW upgrade
5	Hub FPGA FW mismatch
6 -15	Reserved
16	Reference tag battery low
17	Rx does not see reference tag

18	Health tag battery low

Health Status Change Message Upon system status change, may it be because of changes of Current_Health_State, Outstanding_Error_Types or Outstanding_Warning_Types, Dart RTLS system will send out a diagnostic message of type “Health state change” in Dart output data stream. This diagnostic message has syntax as below.

D,Current_Health_State,Latched_Health_State,Outstanding_Error_Types,Outstanding_Warning_Type,0,timestamp,4,”health state changed”

Extended Server Alive Message

Dart RTLS system also extended the existing “Server Alive” diagnostic message to periodically send out system health status. The extended ‘Server Alive” message has following syntax:

D,Current_Health_State,Latched_Health_State,Outstanding_Error_Types,Outstanding_Warning_Type,data_client_count,timestamp,1,”server is alive”

Where data_client_count: total number of currently established data clients (Dart, ISO, or Z-SLMF)

Example:

After a restart the system is in Good state (0)

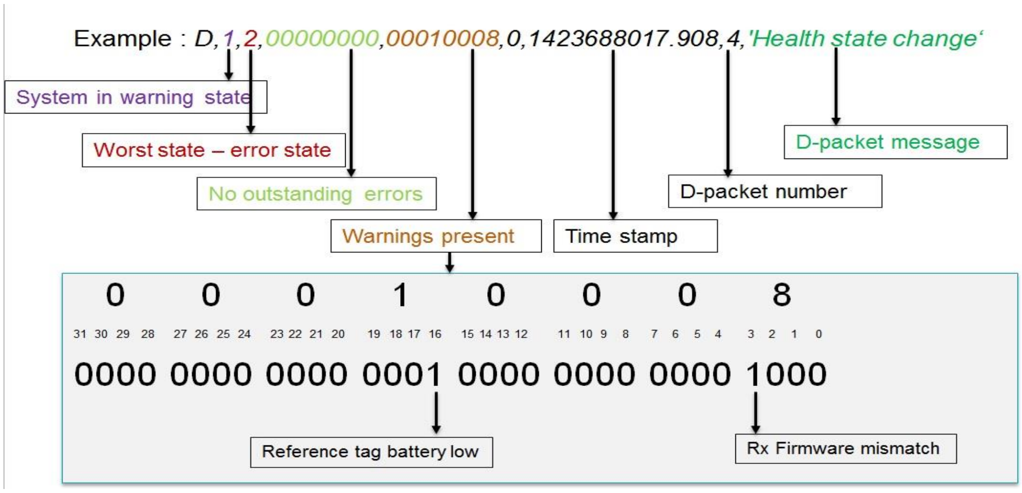
```
•D,0,0,00000000,00000000,2,1423688012.009,1,'Server is alive'
```

Say, a receiver is disconnected from hub. The system health state changes to Error (2)

```
•D,AB,7.0,10.0,8.0,0,1423688017.908,-17,'Error: active receiver communication lost'
•D,2,2,00010000,00000000,0,1423688017.908,4,'Health state change‘
•D,2,2,00010000,00000000,2,1423688073.015,1,'Server is alive'
```

If the receiver is connected back to hub, the system health state changes to good (0) again. But note the latched health state remains as Error (2) as that was the worst state the system experienced.

```
•D,AB,7.0,10.0,8.0,0,1423688094.085,17,'Active receiver communication OK‘
•D,0,2,00000000,00000000,0,1423687072.499,4,'Health state change‘
•D,0,2,00000000,00000000,2,1423688134.019,1,'Server is alive'
```



Example : *D,1,2,00000000,00010008,0,1423688017.908,4,'Health state change'*

Appendix E: Cabling guidelines

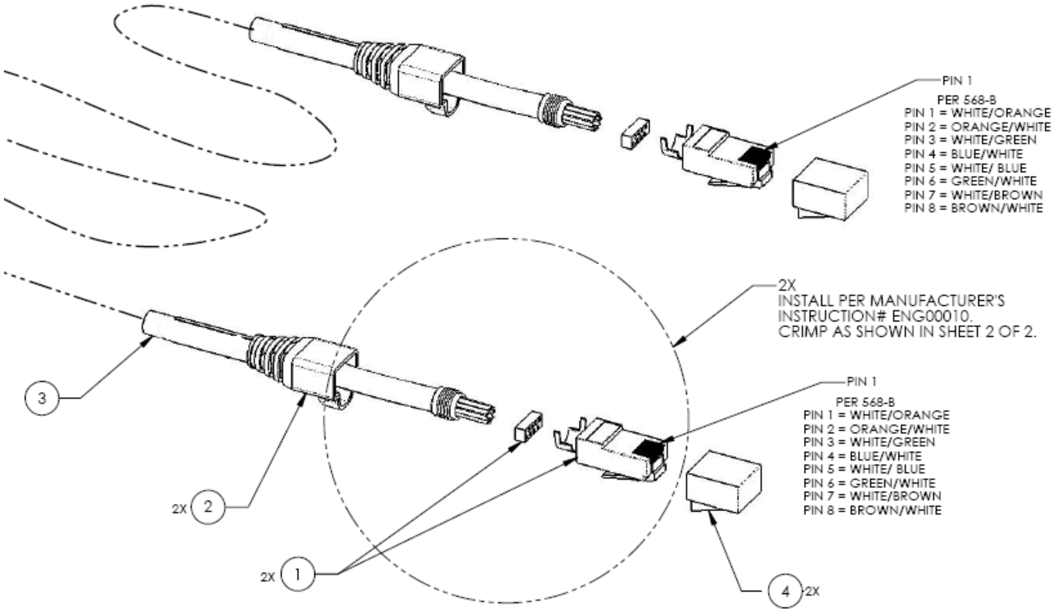
Shielded Cat5E cable assembly recommendations

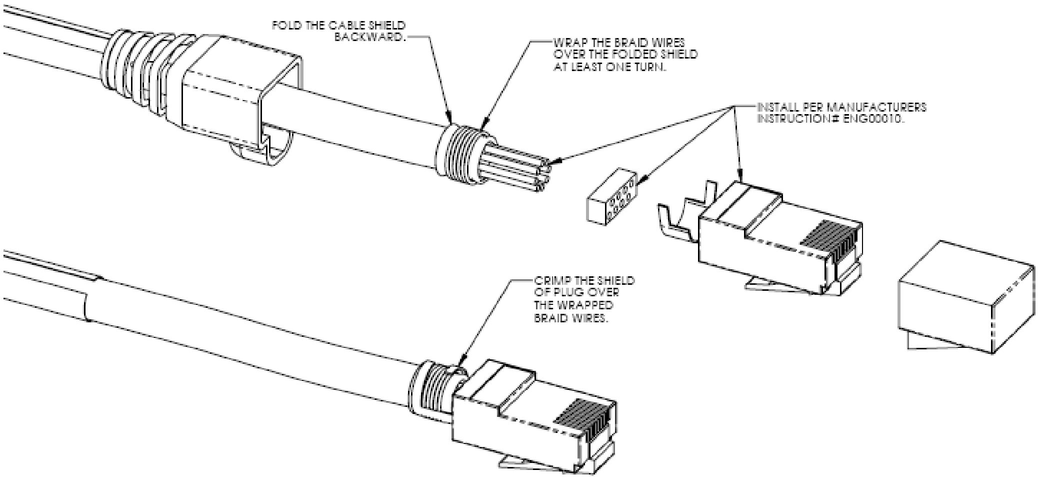
Dart RTLS may use shielded CAT 5E cables with a minimum of 24 AWG. Alternatively, you may use shielded CAT 6E cables and solid cables. You must connect the cable connector to the cable shield.

The following table lists acceptable parts for shielded CAT 5E stranded and shielded 24 AWG cables.

Item Number	Manufacturer	Manufacturer P/N	Description	Quantity
1	Sentinel Connector Systems	111S08080016C34	8 Pin, Shielded CAT 5E Performance Plug	2
2	SPC Technology	SPC14911	Boot, RJ-45 Strain-relief	2
3	Cable Master	CB5033	Cable, CAT 5E Shielded (24 AWG Stranded)	1

The following figures illustrate how to connect the cable connector to the cable shield.



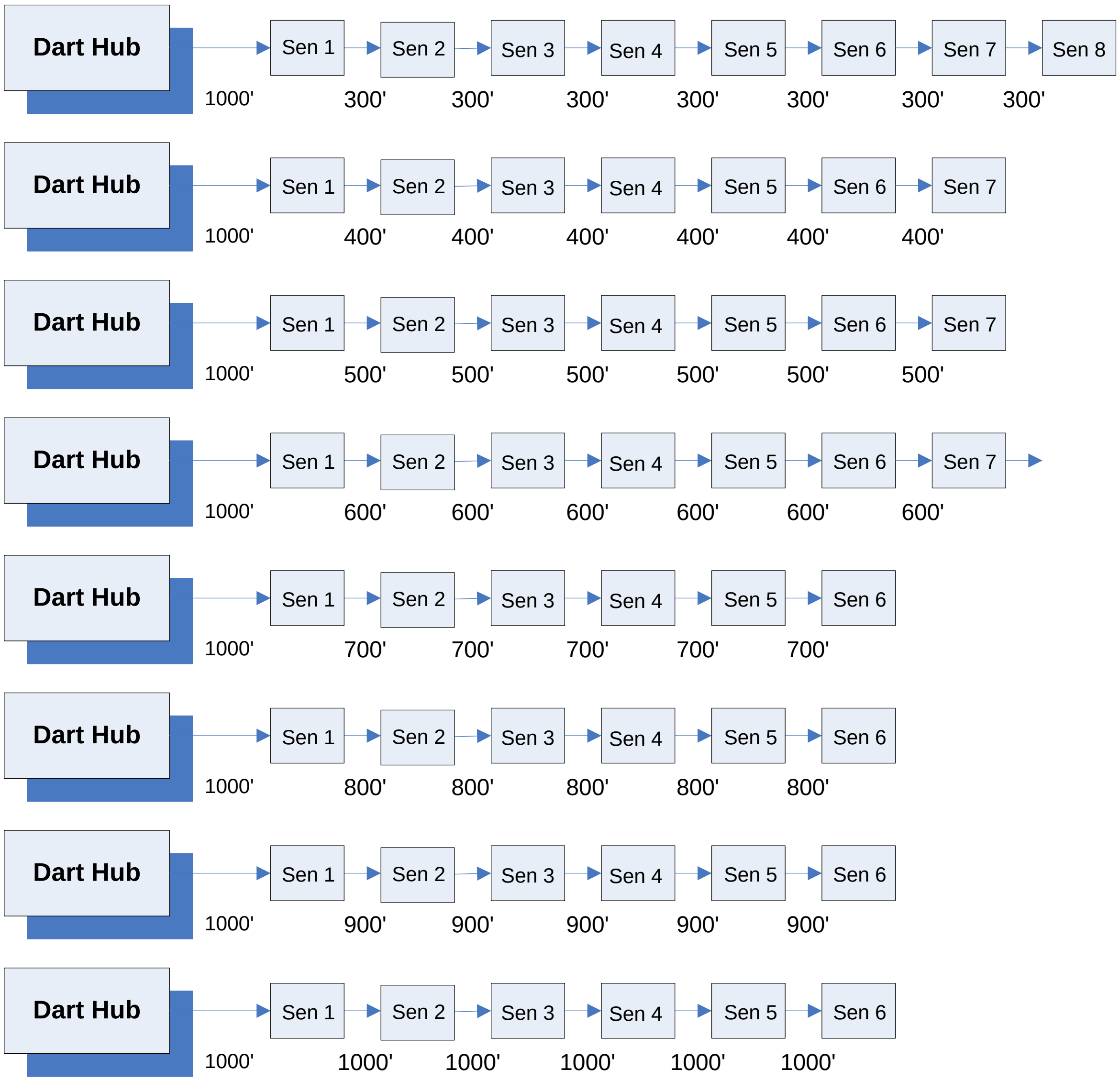

FOLD THE CABLE SHIELD
BACKWARD.
WRAP THE BRAID WIRES
OVER THE FOLDED SHIELD
AT LEAST ONE TURN.
INSTALL PER MANUFACTURERS
INSTRUCTION# ENG00010.
CRIMP THE SHIELD
OF PLUG OVER
THE WRAPPED
BRAID WIRES.

Cable length planning guideline

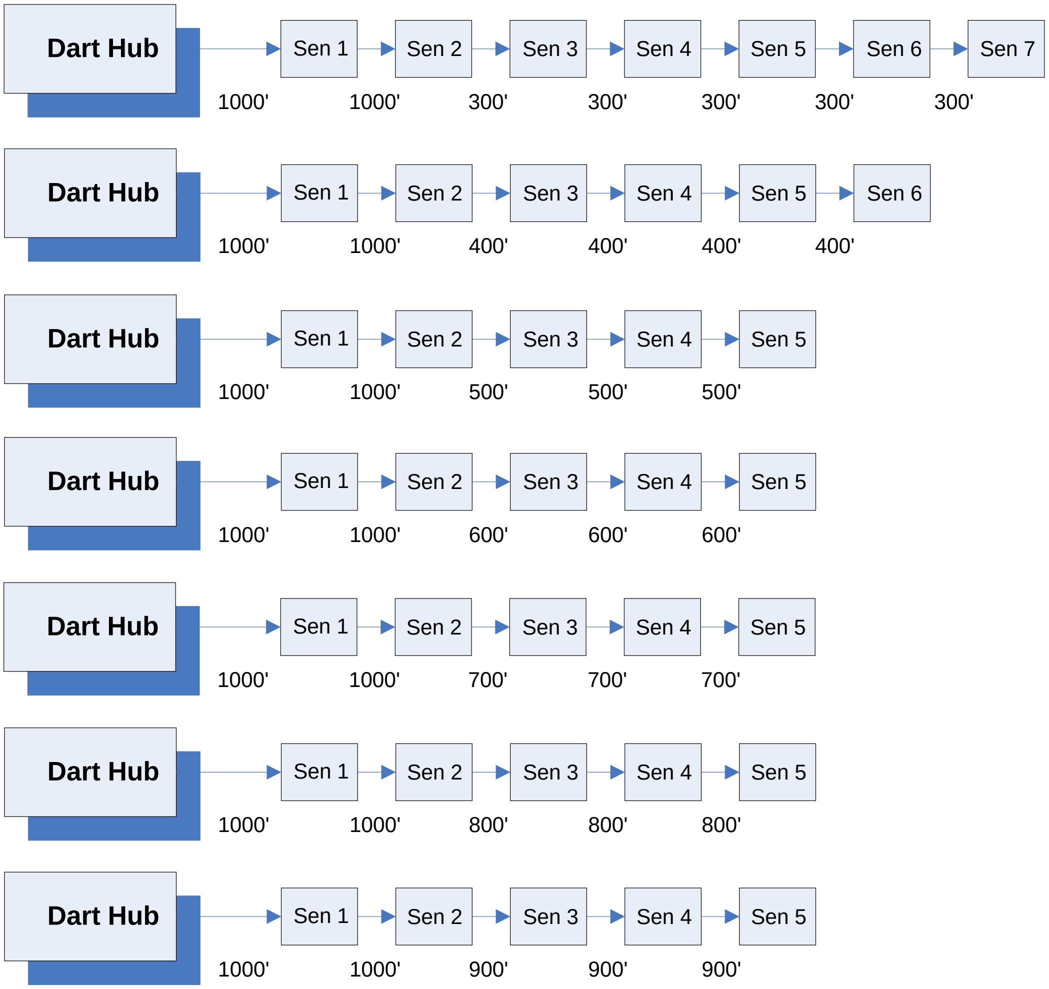
You can connect Receivers directly to a Hub port connection or in a daisy chain to other Receivers. Each Receiver receives 48VDC from the previous Receiver (or from the Hub, if it is the first Receiver in the line) and passes the 48VDC on to the next Receiver in line via the CAT 5E cable. This CAT 5E cable also provides a clock source and serial communication to the Receivers. An external AC adapter can power the Receivers but should only be required with extremely long cable runs.

The maximum hub-to-receiver or receiver-to-receiver cable length is 1000 feet. This section provides guidelines for cable lengths supported without the need for an external AC adapter.

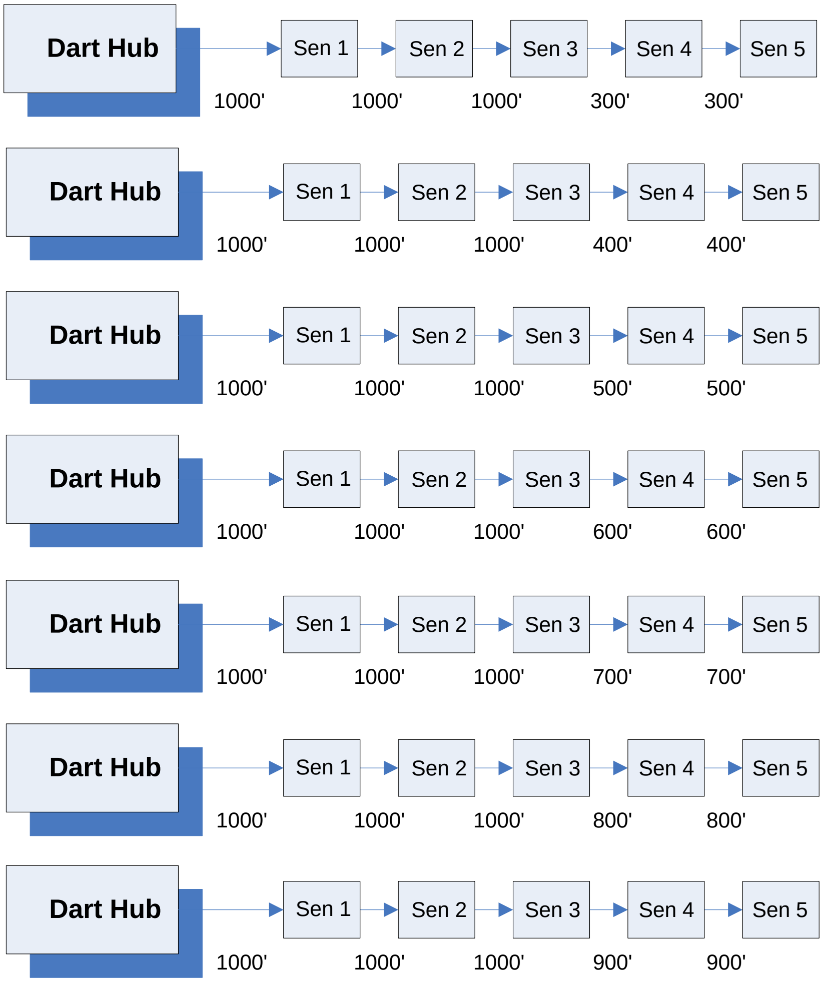
Daisy chain with 1000 feet from the Dart Hub to Receiver 1



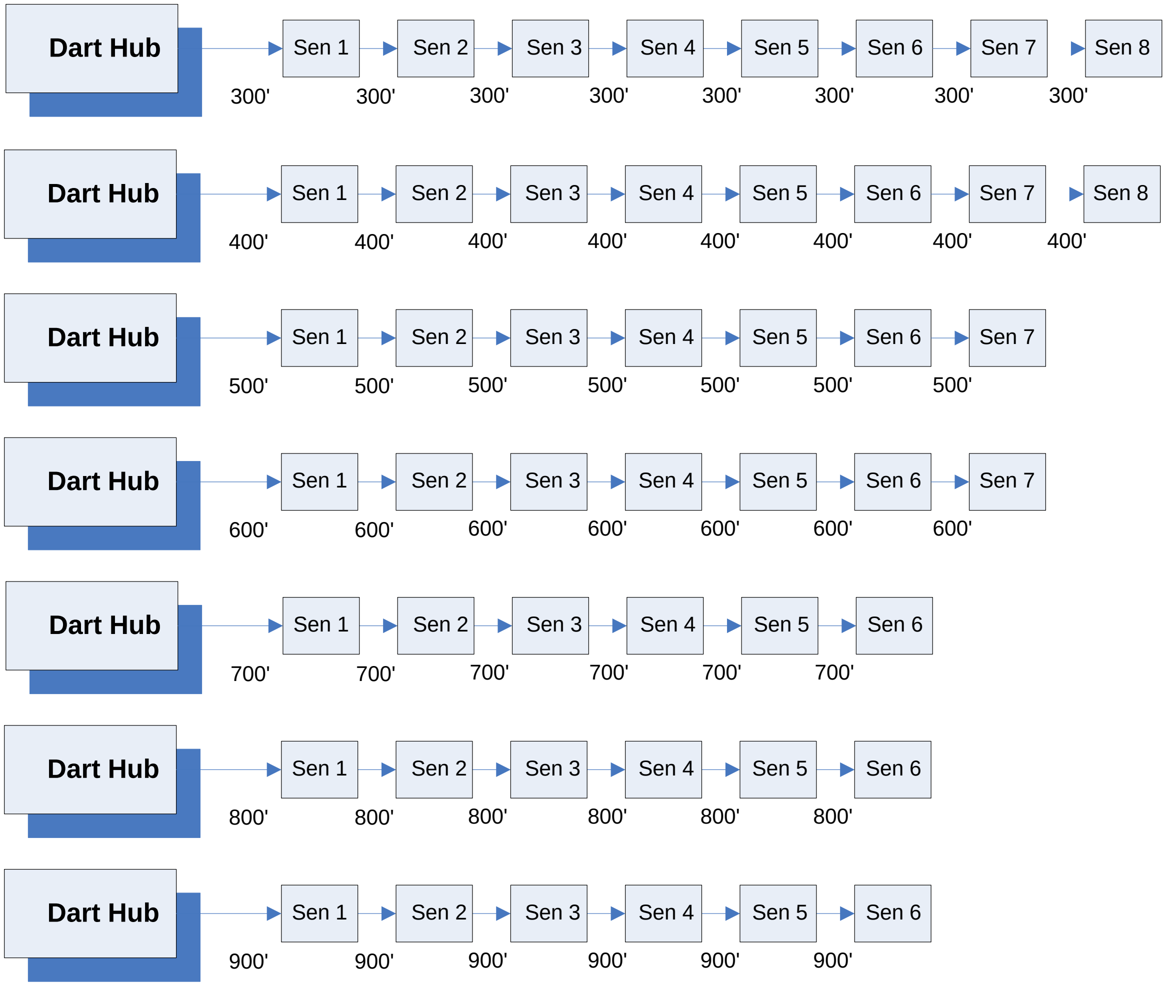
Daisy chain with 1000 feet from the Dart Hub to Receiver 1 and Receiver 1 to Receiver 2



Daisy chain with 1000 feet from Dart Hub to Receiver 1, Receiver 1 to Receiver 2, and Receiver 2 to Receiver 3


Dart Hub → Sen 1 → Sen 2 → Sen 3 → Sen 4 → Sen 5
1000' 1000' 1000' 300' 300'
Dart Hub → Sen 1 → Sen 2 → Sen 3 → Sen 4 → Sen 5
1000' 1000' 1000' 400' 400'
Dart Hub → Sen 1 → Sen 2 → Sen 3 → Sen 4 → Sen 5
1000' 1000' 1000' 500' 500'
Dart Hub → Sen 1 → Sen 2 → Sen 3 → Sen 4 → Sen 5
1000' 1000' 1000' 600' 600'
Dart Hub → Sen 1 → Sen 2 → Sen 3 → Sen 4 → Sen 5
1000' 1000' 1000' 700' 700'
Dart Hub → Sen 1 → Sen 2 → Sen 3 → Sen 4 → Sen 5
1000' 1000' 1000' 800' 800'
Dart Hub → Sen 1 → Sen 2 → Sen 3 → Sen 4 → Sen 5
1000' 1000' 1000' 900' 900'

Daisy chain with equal cable length between Hub and Receivers



Appendix F: Air Filter Maintenance

This section includes information on air filter replacement and cleaning for UWH-1200 hub

1) Filters are to be replaced or cleaned when they are visibly dirty. When replacing or cleaning filter, Hub does not need to be turned off as long as this operation is completed within ½ hour.
2) To remove filter, remove 4 thumb screws (use a Philips screw driver to remove if needed) and detach frame from hub. Remove the dirty filter from the frame.

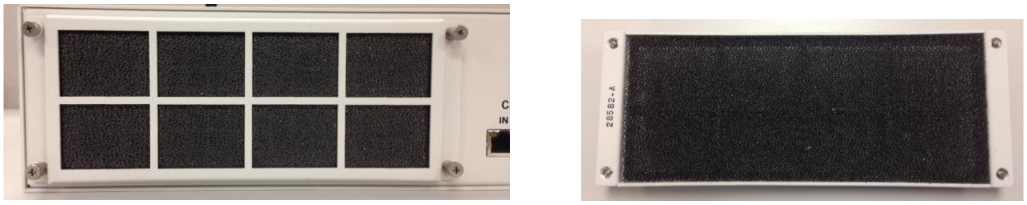


Figure 1. Removing filter from Hub

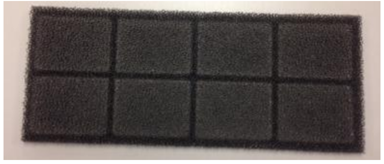


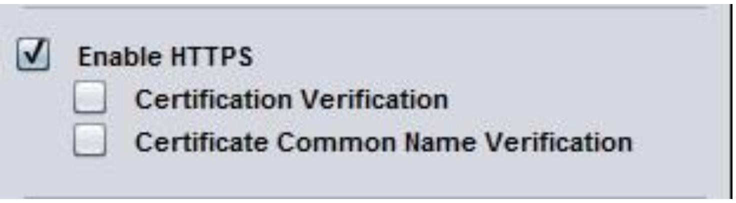
Figure 2. Dirty filter

3) Replace with new filter or Clean the dirty filter by using a vacuum cleaner or wash with water and mild soap removing dust and dirt. Make sure to dry the filter before assembling.
4) Place filter in frame and assemble back into unit, thumb screw only need to be hand tight.
5) A set of two filters can be ordered with the part number UAC-100-00.

Appendix G: HTTPS Support

Dart Hub now provides better HTTPS support to establish secure connection. In the process of establishing HTTPS connection to the hub, some verification can be enabled or disabled from Zebra Hub Manager (for Hub FW version 5.0.0 and up). The following fashions of HTTPS connection are supported by Dart Hub and Zebra Hub Manager.

HTTPS Only

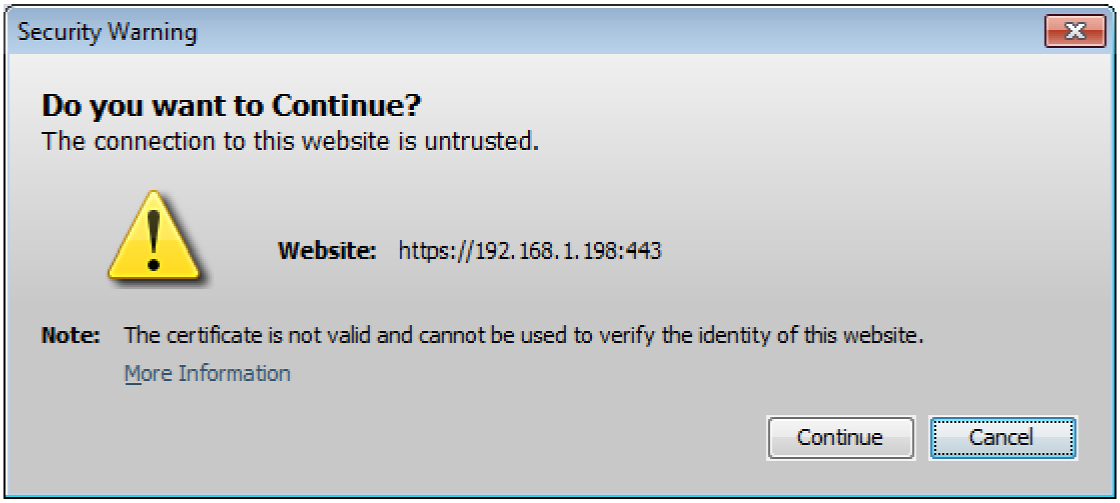


☑ Enable HTTPS

□ Certification Verification

□ Certificate Common Name Verification

In this fashion, certificate verification and certificate common name verification are both disabled. Any valid X.501 certificate, from trusted certificate authority (CA) or self-signed, is trusted, and is used to establish secure connection. Dart hub is shipped with a self-signed certificate residing inside the hub. Therefore, the user does not need to do anything to securely access the hub in this fashion. When connecting, following security warning may appear.



Security Warning

Do you want to Continue?
The connection to this website is untrusted.

Website: https://192.168.1.198:443

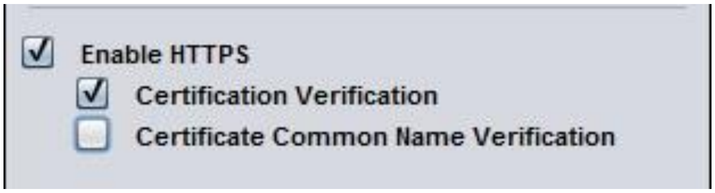
Note: The certificate is not valid and cannot be used to verify the identity of this website.

Select

Continue when it appears.

To enable the HTTPS only mode In profile settings using Zebra Hub Manager, check **Enable HTTPS**, uncheck **Certificate Verification** and **Certificate Common Name Verification**.

HTTPS with certification verification

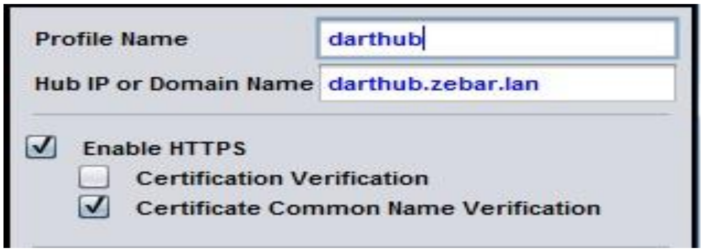


☑ Enable HTTPS
☑ Certification Verification
□ Certificate Common Name Verification

When establishing secure connection in this manner, Zebra Hub Manager will obtain the whole chain of certificates used by the hub, verify it to make sure the certificates are properly signed, and the whole certificate chain can be traced back to a trusted CA, In this mode, the common name of the hub certificate is not checked against the hub domain name.

Since the self-signed certificate originally shipped with Dart Hub won't pass the verification, before connecting to the hub in this mode, the user need to obtain a valid certificate from a trusted CA, and upload it to the hub. Refer to *Upload Certificate to Hub* for more details on uploading certificate. If the trusted CA that issues hub certificate is not well trusted, the user can enforce the trust by uploading the CA certificate to Zebra Hub Manager, as detailed in *Upload CA Certificate to Zebra Hub Manager*

HTTPS with certificate common name verification



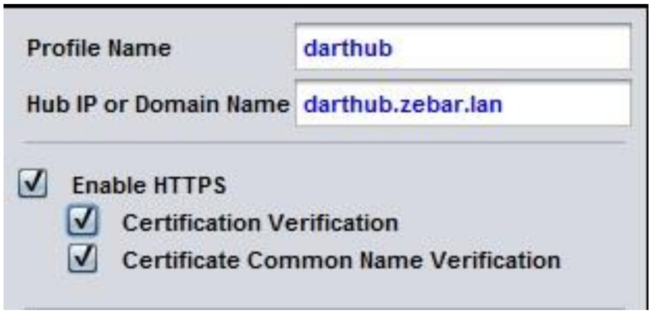
Profile Name darthub
Hub IP or Domain Name darthub.zebar.lan

☑ Enable HTTPS
□ Certification Verification
☑ Certificate Common Name Verification

This mode of secure connection requires Dart Hub obtaining a valid X.501 certificate, from trusted CA or self-signed, with certificate common name matching the hub's domain name. To establish secure connection in this manner, a fully qualified domain name needs to be assigned to the Hub, and a certificate with common name as the assigned domain name needs to be created and uploaded to the Hub. Refer to *Upload Certificate to Hub* for more details on uploading certificate.

To enable this type of secure connection, in the profile settings in Zebra Hub Manager, input the fully qualified domain name in **Hub IP or Domain Name** box, check **Enable HTTPS**, uncheck **Certificate Verification,** and check **Certificate Common Name Verification**.

HTTPS with certificate verification and common name verification



Profile Name: darthub

Hub IP or Domain Name: darthub.zebar.lan

☑ Enable HTTPS

☑ Certification Verification

☑ Certificate Common Name Verification

This mode is the most secure one since it requires both certificate verification and certificate common name verification, as outlined in the above two sections. To use this mode, the Zebra Hub needs a fully qualified domain name, and a valid X.501 certificate with common name as hub's domain name obtained from a trusted CA and upload it to the Zebra hub. The user needs to upload the certificate to the Hub, and optionally, upload the CA certificate to Zebra Hub Manager.

To connection hub in this manner, in the profile settings, input the fully qualified domain name in **Hub IP or Domain Name** box, check **Enable HTTPS**, **Certificate Verification,** and **Certificate Common Name Verification.**

Uploading certificate to Zebra Hub

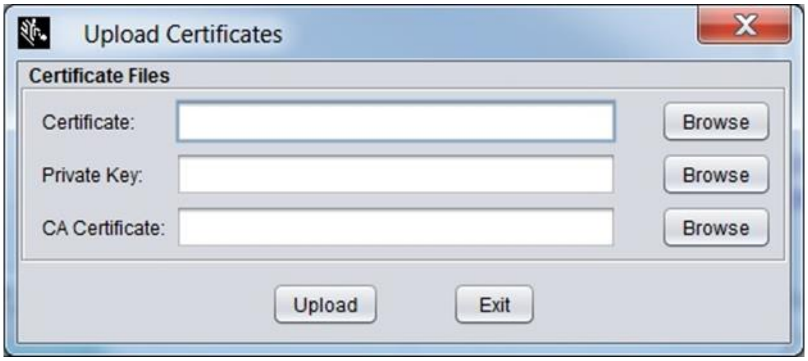
1 Based on the format the certificate is created, it can be as one file or several files. Before uploading the certificate to the hub, the user may need to covert received certificate into three files:

- Hub certificate in PEM format
- CA certificate contain the whole certificate path from hub certificate issuer to a trusted CA in PEM format
- unencrypted private key in PEM format

2 Start Hub Administration and Management application, and click **Administration** to enter **Sign In** tab of Administration page.

3 If the hub is configured to use **Open Access** mode, Select **Sign In Based Access** in the **System Access Control** in Main tab, and click **Save** to enable and enter **Sign In** tab.

4 Click **Upload Certificates.**

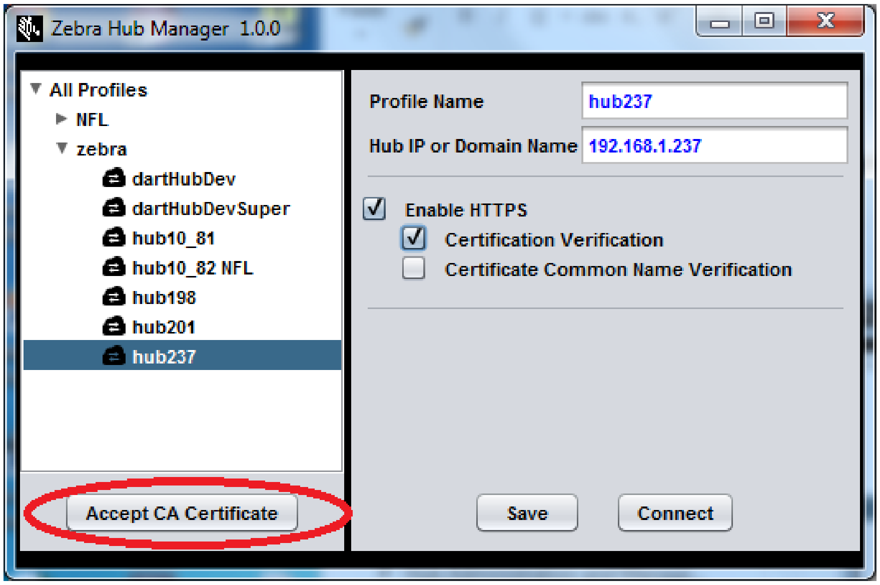


5 Browse or input the path to three certificate files as list in step 1.

6 Click **Upload.**

Uploading CA certificate to Zebra Hub Manager

1 On Zebra Hub Manager, click on **Accept CA Certificate**, browse to the location where the CA certificate exists and click Load.



Profile Name hub237

Hub IP or Domain Name 192.168.1.237

☑ Enable HTTPS

☑ Certification Verification

☐ Certificate Common Name Verification

Regulatory Information

This section includes regulatory information for:

- ***Canada*** *(on page 142)*
- ***U.S.*** *(on page 142)*
- ***EU*** *(on page 143)*

Canada regulatory information

The hub and receivers comply with CAN ICES-3(A)/NMB-3(A). The tags comply with RS-220 and RSS-GEN. Refer to document number D1685 for additional details for the tags.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada

U.S. regulatory information

The tags comply with FCC Part 15.250 (c). Refer to document number D1685 for additional details for the tags.

Note

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

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

RF Notice

Any changes or modifications to Zebra Enterprise Solutions (ZES) equipment not expressly approved by ZES could void the user's authority to operate the equipment.

EU regulatory information

Refer to document number D1685 for details for the tags.

Specifications

This section lists specifications for Dart UWB RTLS.

Dart RTLS General Specifications

Mode of Operation	Precision relocation using time-differences of arrival
Accuracy	± 1 foot (without signal averaging) ± 4 inches (with signal averaging)
Maximum number of Receivers per Hub	64
Data throughput per Receiver high-speed pair	2.0 Mb/s
Maximum distance between RX#1 and Hub	1000 feet*
Maximum number of Receivers per daisy chain	8
Maximum number of reference tags supported per Hub	32
Number of virtual groups supported by one Hub	32

* Using a 24AWG CAT 5E cable (or better)

Dart Hub Specifications*

Model	**UWH-1200**
Performance	
Data Throughput	Up to 7000 1 Hz tags/second
Tag Capacity	Up to 10,000 tags/hub
Environmental/Physical	
Operating Temperature	0ºC to 40ºC (32ºF to 104ºF)
Dimensions	42 cm x 32.5 cm x 8.5 cm (16.5 in. x 12.8 in. x 3.3 in.)
Weight	5 kg (11 lbs)
Power	100 – 240 VDC 50/60 Hz; 3.15 A Provides power for up to 64 Receivers

Model	UWH-1200
Ports	Power 2- RJ45 Ethernet ETH0 & ETH1 (ETH1 is not used) 8 – RJ45 (Clock, Data & Power to Receivers) 2 –RJ45 (clock in & clock out currently not used) 1- RS232 – This connector is a host male connector, in order to connect to a computer which will be a host as well, a female to female null cable is required (such as L-com CSNULL9FF-5A WWW.L-COM.COM)

Dart Receiver Specifications*

	High Gain	Mid Gain	Omni	Bulkhead
Model	UWC-1100	UWC-1200	UWC-1300	UWC-1400
Frequency Range	6.35 to 6.75 GHz	6.35 to 6.75 GHz	6.35 to 6.75 GHz	6.35 to 6.75 GHz
Antenna Gain	14 dBi	7.5 dBi	4.5 dBi	N/A
Environmental/Physical				
Operating Temperature	-40ºC to 70ºC (-40ºF to 158ºF)	-40ºC to 70ºC (-40ºF to 158ºF)	-40ºC to 70ºC (-40ºF to 158ºF)	-40ºC to 70ºC (-40ºF to 158ºF)
Environmental Rating	IP40	IP40	IP40	IP40
Dimensions	15.5 x 6.4 x 7.1 cm	15.5 x 6.4 x 7.1 cm	25.4 x 6.4 x 7.1 cm	16 x 6.4 x 7.1 cm

* Specifications are subject to change without notice.

Zebra customer support

All Dart RTLS documentation and firmware updates (including the Dart RTLS User Manual) may be downloaded from the Customer Portal. After logging into the Customer Portal, click on "Content" from the menu bar, select "Dart UWB (Current Customers)" from the "Search In" drop-down list, then press "Go!"

If you are a first-time Customer Portal user, you can obtain a user name and password by following these steps:

1. Go to the Zebra Support Center Login page: http://www.zebra.com/us/en/forms/support-center-login.html.
2. Click on the "Not a registered user" link on this page.
3. Click on the "Register" link on the new page.
4. This will open a form which should be completed and submit.
5. This form is forwarded to the Customer Support Team. Upon approval, an acceptance e-mail with a Login Name and Password will be sent back to the customer-supplied e-mail address.

Should you have any questions about the website, product content, or access to such, please contact the Customer Support Group by sending an email to ZES.support.LS@zebra.com.