Certification Exhibit

FCC ID: S4MGRG3-18-B

FCC Rule Part: 15.247

ACS Report Number: 09-0230-15C

Manufacturer: **TeraHop Networks, Inc.**
Model(s): **GR2100a**

Manual

TeraHop networks™

IMS Installation and Operation Manual V1.1

Table of Contents

Figures

Tables

Revision History

Revision	Date	Changes Made
1.0	May 2009	
V1.1	July 20, 2009	See the Release Notes

TeraHop Networks Incident Management System (IMS) *with* Automated Accountability Installation and Operation Manual V1.1

TeraHop Document Number 08-00008-01

FCC Statement for Electromagnetic Interference:

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

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

FCC Statement for Exposure for RF Exposure Limits:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Statement for Part 15.21 Compliance:

Warning: Changes or modifications to this device not expressly approved by Terahop Networks, Inc. could void the user's authority to operate the equipment.

1225 Old Alpharetta Rd., Suite 210
Alpharetta, GA 30005
http://www.terahop.com

1.0 Introduction

This is the Installation and Operation manual for the **TeraHop™ Incident Management System (IMS)** ***with*** **Automated Accountability**. This system is comprised of Remote Sensor Nodes (RSNs), a Gateway Router (GR), a Gateway Server (GS), a Message Management and Routing (MMR) System, and Personal Digital Assistants (PDAs).

The TeraHop IMS is a powerful tool used to manage and record assets and events utilized by First Responders in the performance of their duties at an incident site. The system is a collection of purpose-built electronic components and application software. When deployed, an Incident Commander (IC) is given powerful visibility and monitoring capabilities of multiple on-scene assets literally in the palm of his/her hand.

This manual provides the instructions necessary for trained equipment personnel to effectively install and verify its operation and perform routine maintenance. Keep in mind that this manual supports these activities for approved TeraHop Networks (THN) Field Technicians and authorized partners only. Normal activities performed by end users (customers) are covered in other THN documents and are considered outside the scope of this document. Any referenced field repair is limited to the replacement of equipment that has been designated as "field replaceable."

You are always encouraged to contact TeraHop Networks Customer Service directly if you encounter any difficulties in executing the procedures outlined in this document.

The TeraHop RSN described in this manual complies with FCC requirements per the statement below:

FCC ID: S4MRSN300-06-B THIS DEVICE COMPLIES WITH PART 15 OF THE FCC RULES. OPERATION IS SUBJECT TO THE FOLLOWING TWO CONDITIONS:

(1) THIS DEVICE MUST NOT CAUSE HARMFUL INTERFERENCE, AND

(2) THIS DEVICE MUST ACCEPT ANY INTERFERENCE RECEIVED INCLUDING INTERFERENCE THAT MAY CAUSE UNDESIRED OPERATION.

The TeraHop Gateway model GR2100a described in this manual complies with FCC requirements per the statement below:

FCC ID: S4MGRG3-18-B THIS DEVICE COMPLIES WITH PART 15 OF THE FCC RULES. OPERATION IS SUBJECT TO THE FOLLOWING TWO CONDITIONS:

(1) THIS DEVICE MUST NOT CAUSE HARMFUL INTERFERENCE, AND

(2) THIS DEVICE MUST ACCEPT ANY INTERFERENCE RECEIVED INCLUDING INTERFERENCE THAT MAY CAUSE UNDESIRED OPERATION.

2.0 Use of This Manual

This manual contains the information necessary to support installation and operation activities that are to be performed by THN Field Service Technicians and affiliated Channel Partners (CPs). Specific procedures can be located in the Table of Contents, which references a page number for each procedure contained in the manual.

In terms of field repair, the manual contains fault isolation procedures that reference specific maintenance tasks. Execution of the recommended task will be followed by a Performance Verification procedure. This procedure will verify that the unit has been returned to a fully-operational state.

Conventions Used in This Manual

When using this manual, you will note that some words and terms are in bold. Items that are in bold are items that you enter, select, or click on a screen. Other important terms and cautions are also in bold. For example:

To configure sectors/divisions, do the following:

1. Click the **Sectors/Divisions** icon.
   The **Sector Division List** screen appears displaying the rows and columns for data to enter for each record in the sector/division database. The application table shown below is pre-populated with default values. These defaults can be used, edited, or deleted using this table.

Messages that appear on the screen are in italics. For example:

To delete a record, select the record and click the **Delete** icon. The following message appears: *Are you sure you want to delete xxx?*

Unless specified otherwise, all references or links to other topics direct the reader to topics within this manual.

Unless specified otherwise, when instructed to click an item on a screen, for right-handed mouse users, it is a single left-click on the mouse.

3.0 Overview of the Contents of This Manual

The following paragraphs describe the sections of this manual.

Hardware Installation and Setup

Software Installation and Setup

Using the IMS Software: The TeraHop Console

Configuring the IMS Application

Configuring Remote Sensor Nodes (RSNs)

Operational Checkout and System Commissioning

Warranty, Technical Support, and Returning Equipment

Vendor Data Sheets

Spare Parts Recommended List

Tool Set

System Component Specifications

4.0 IMS Installation Process

4.1 Overview

The following describes the process to install the IMS. Instructions for completing each step in the process are described in the IMS Implementation Notebook and/or the IMS Installation and Operation Manual.

The system is manufactured with the current firmware and software versions and default First Responder settings.

The default Customer ID is installed by the manufacturer into the Message Management and Routing (MMR) System.
The Area ID (AID) is installed by the manufacturer into the Gateway Server (GS).

The system is shipped to the Channel Partner and includes:

- Gateway Router (GR)
- Gateway Server (GS)
- Personal Data Assistants (PDAs)
- Remote Sensor Nodes (RSNs) (in deep sleep mode)
- Message Management and Routing (MMR) System
- Ethernet switch
- Mobile Gateway Cable Installation Kit
- Administration Station (ADMS) laptop computer with TeraHop Console (THC) software, TeraHop Data Transfer (TDX) software, IMS Application Configuration Tool (ACT) software, RSN Configuration Viewer (RCV) software, and RSN Configuration Tool (RCT software. User guides for these tools are available for download from the TeraHop Networks Customer Relationship Management (CRM) System. For more information, contact TeraHop Networks Customer Service via e-mail or by calling 770-663-3455.

The installer provides the following:

- Crimp connectors
- Barrier strips
- Mounting kits
- Crimps
- High-power on/off switch
- Mounting materials

To install the IMS hardware and software, follow the process outlined below.

- Using the RCT, wake up one RSN. (See How to Wake Up an RSN in this manual.)
- Using the RCT, program one RSN with the customer ID. (See How to Configure RSNs in this manual.)
- Perform a System Bench Check: hook up the system with all hardware connected using a 12V power supply. You can do a system bench check with the factory defaults. It should show up with a customer ID of 70. (See Operational Checkout and System Commissioning in this manual.)
- Configure the real Customer ID (as assigned by TeraHop Networks) in the MMR. (See How to Edit the Customer ID and AcceptFirstResponder Options in the MMR in this manual.)
- Configure the Wi-Fi SSID on the GR. (See Updating the Gateway Router Access Point Configuration in this manual.)
- Update the PDA Wi-Fi with access point SSID – update the Config File. (See Updating the PDA Software, Step 3 Set PDA System Configuration and Wi-Fi SSID in this manual.)
- Configure the PDA with sectors/divisions, profiles, and incident types using the ACT. (See Configuring the IMS Application in this manual.)
- Configure the rest of the RSNs with configurations (parameters) and user data. See Configuring RSNs in this manual).
- Download RSN configurations to the RSNs. (See Configuring RSNs in this manual.)
- Configure the Administration Station (ADMS) with Wi-Fi SSID (see Setting the ADMS SSID to Connect to the Mobile Gateway System (MGS)).
- Retest the entire system on the bench.
- Install the system in the vehicle. (See Hardware Installation in this manual.)
- Test in the vehicle – run the operational checklist procedure. (See Operational Checkout and System Commissioning in this manual.)

5.0 Hardware Installation and Setup Introduction

5.1 Hardware Installation and Setup Guidelines

This section provides guidelines that should be taken into consideration whenever a system is going to be placed in the field. Every set of circumstances will be different; therefore, it is impossible to provide step-by-step instructions. There are however certain activities that must be accomplished in every instance regardless of the details of the fielding, these are;

- A site survey should be conducted on a pre-sales basis
- Upon delivery and prior to the start of any installation activities, a thorough inventory of equipment should be performed. Any missing hardware should be addressed with TeraHop Networks Customer Service immediately.
- All indoor equipment shall be installed in an area that provides adequate protection from the environment.
- All outdoor equipment shall be installed in a manner that considers not only the environment, but vehicle use, the terrain of the operational area, and obstacles that will likely be encountered during day-to-day use of the vehicle.

5.2 Equipment Description and Purpose

The TeraHop Incident Management System (IMS) *with* Automated Accountability solves problems related to personnel accountability and incident-management effectiveness. Incident Commanders (ICs) are faced with the daunting task of remaining cognizant of Emergency Services Sector (ESS) assets as they enter and leave an incident scene.

This routine entry and exiting at a site is often the result of assets responding to call-outs. Additionally, each asset brings skill sets that are often particular to that specific asset. As assets come and go and situational changes occur in the area, this continuous accounting of assets can be invaluable.

The IMS also requires very little in terms of manual set-up time and reduces mindshare time to a minimum prior to actually being able to manage the assets at an incident in real-time. The system also is a valuable aid after the incident is resolved when creating/preparing official reports.

The following paragraphs explain at a very high level how the various components in the First Responder system work together to provide these tactical tools to the IC.

5.2.1 Remote Sensor Nodes

TeraHop Remote Sensor Nodes (RSNs) are an element of TeraHop's moveable, wireless, sensor networks that provide timely asset and incident resource management and data.

Each asset (each First Responder, piece of equipment, or vehicle) is supplied with an RSN. If there are 7 assets in the situational area, then the network will be made up of 7 RSNs; if there are 34 assets in the situational area, then the network will be made up of 34 RSNs and so forth.

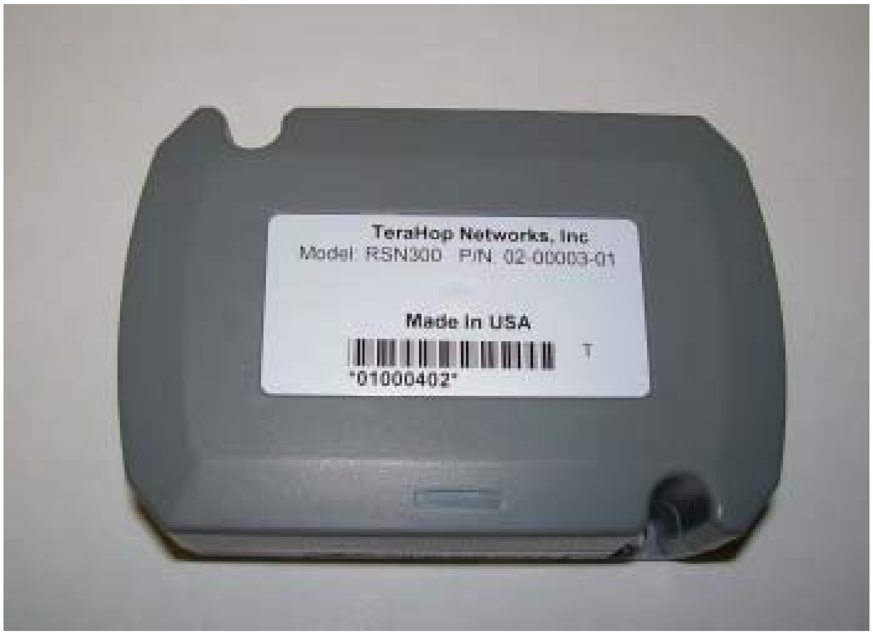


Figure 1: RSN Front

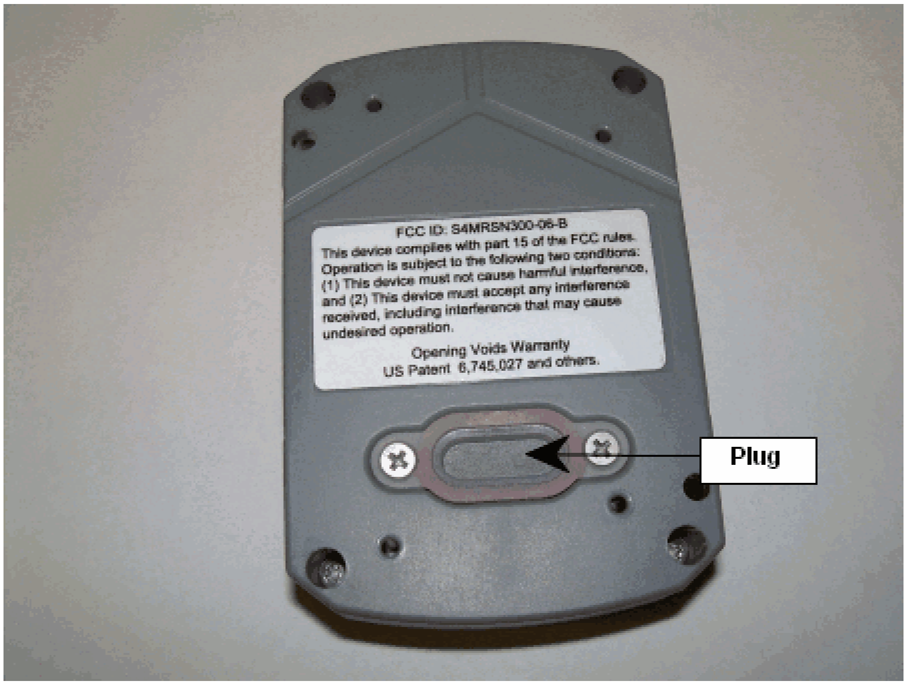

FCC ID: S4MRSN300-06-B
This device complies with part 15 of the FCC rules.
Operation is subject to the following two conditions:
(1) This device must not cause harmful interference,
and (2) This device must accept any interference
received, including interference that may cause
undesired operation.
Opening Voids Warranty
US Patent 6,745,027 and others.
Plug

Figure 2: RSN Back

The RSNs are small, battery-powered devices that may be affixed to equipment or vehicles, or carried by people that one wishes to monitor. RSNs also incorporate a variety of sensors including configurable motion and shock detection that can monitor changes in the resource's condition and/or status. RSNs have an expansion port for connecting to external sensors and monitoring devices.

When one or more RSNs come within range of a TeraHop Gateway, they form a wireless network referred to as an island. RSNs exchange data with each other and with Gateways over the worldwide-allocated 2.4 GHz radio spectrum. RSNs will forward sensor data based upon internal, customer-defined profiles. Information from one RSN can be forwarded from one device to another until the message reaches its target destination.

TeraHop RSNs can be configured with asset-specific data such as the wearer's name, special skills, or a fire engine number, a company name, etc. In addition to reporting data autonomously, RSNs can be queried for their status and settings.

5.2.2 TeraHop Gateway Routers

The TeraHop Gateway Router, hereafter referred to as the GR or simply the Router, functions as a network edge device in the TeraHop IMS network. It can be thought of as a combination replay/media converter. It functions as a relay by providing backhaul network capability for other GR and RSN devices to the Gateway Server and as a media converter by translating IP-based messages to proprietary reduced complexity radio and Bluetooth radio protocols. The Gateway Router's primary function is to exchange sensor data and event messages between RSN devices and the TeraHop Gateway Server. Additionally, it provides Wi-Fi connectivity between the PDA and application.

Figure 3: Gateway Router

5.2.3 Gateway Server

The Gateway Server (GS) is responsible for site management, providing Domain Naming Service (DNS) and Dynamic Host Configuration Protocol (DHCP) services for all computers that attach (GR, MMR, PDA). The GS also acts as a buffer for all events from the RSNs to guarantee delivery to the MMR.

Figure 4: Gateway Server

5.2.4 Message Management and Routing System

The MMR provides a variety of functionality for the IMS, including governing what RSNs should and should not be allowed on the network, monitoring the presence of RSNs so that the user can be notified if an assigned RSN goes out of contact, collecting RSN message data for post-incident analysis, and troubleshooting and hosting the IMS application itself.

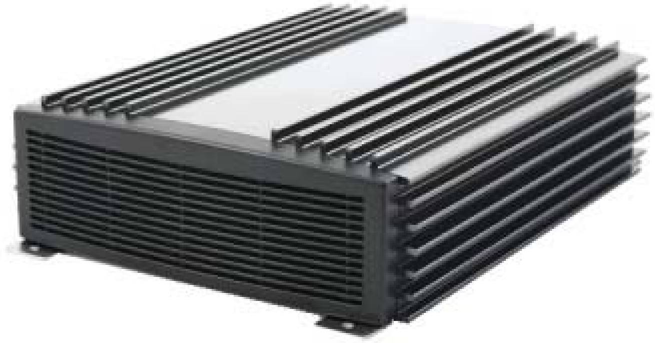


Figure 5: Message Management and Routing System

5.2.5 Administration Station (ADMS)

The Administration Station is an 802.11a Wi-Fi-equipped laptop computer used for the configuration of RSNs and the retrieval of incident logs. This laptop is typically left at the station and not on board the command vehicle.

Figure 6: Administration Station (ADMS) Laptop Computer

5.2.6 RSN Configuration Tool (RCT) Cradle

The RCT Cradle is used with the ADMS to configure and verify RSN devices. Aside from serving as an adapter between the RSN and the ADMS, the RCT contains diagnostic LEDs to help verify operation and diagnose issues.

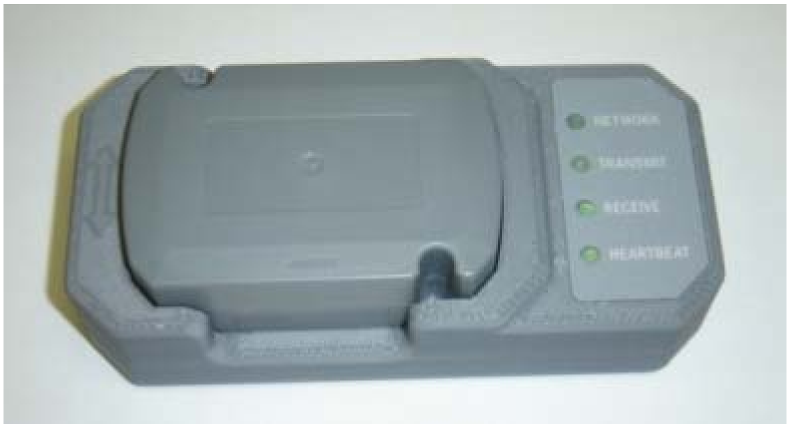


Figure 7: RCT Cradle and RSN

5.3 Incident Management System (IMS) Operational Description

The Incident Management System with Automated Accountability enhances and automates key personnel tasks for the Incident Commander. TeraHop's IMS detects the presence of individual personnel and units automatically and passes the data to the Incident Commander's hand-held personal digital assistant (PDA). The System is made up of just a few components:

- Mobile Gateway System (MGS)[1]
- PDA with Incident Management software, and
- Remote Sensor Nodes (RSNs).

An MGS is installed on major pieces of equipment, such as the Incident Commander's vehicle.

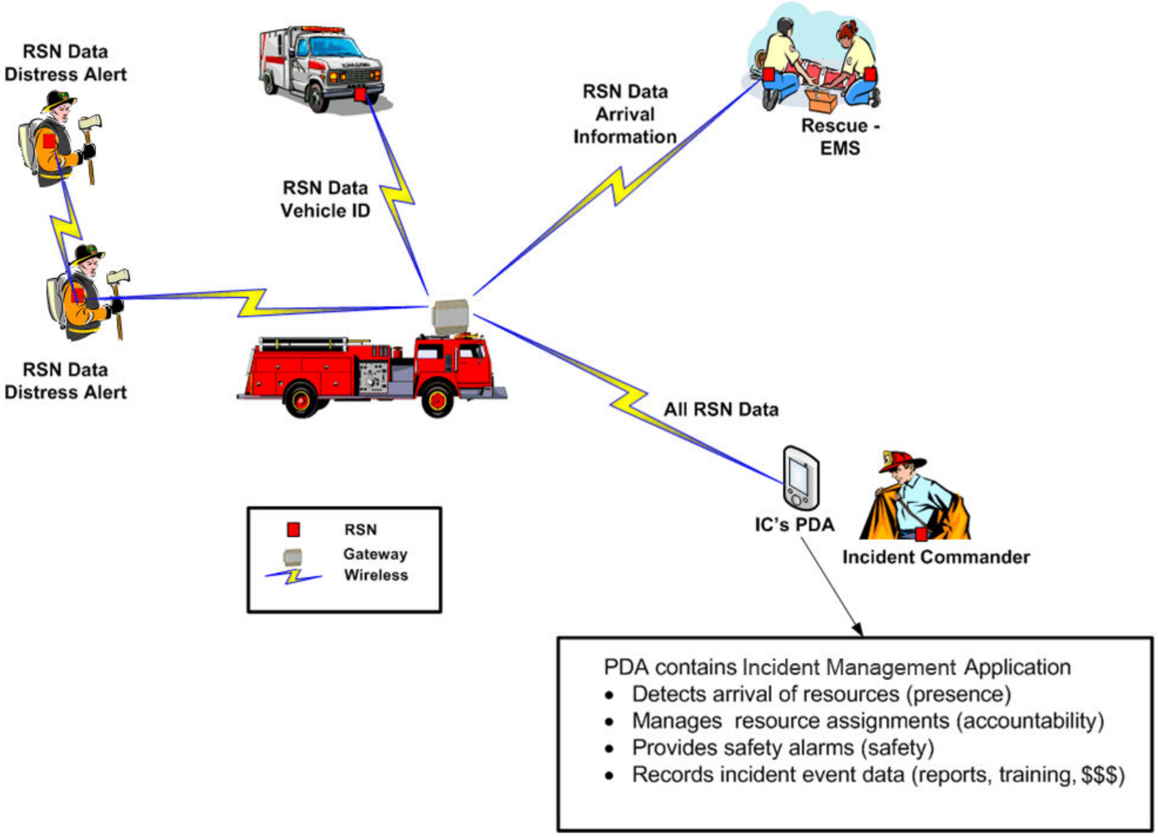
The RSNs are attached to units and equipment and are worn by personnel.

The IMS application software resides in the MMR System and is accessed from the Incident Commander's hand-held PDA.

When the system components are in RF range, they form a wireless network island around the incident scene. This network island expands and contracts as units, equipment, and personnel arrive and leave the incident scene. TeraHop's IMS helps to relieve the Incident Commander of several accountability tasks, thereby making it easier and quicker

[1] An MGS is the combination of a GR, MMR, and GS installed on a mobile platform.

to complete them. A detailed incident report is automatically generated at the conclusion of each incident using the IMS.



PDA contains Incident Management Application

- Detects arrival of resources (presence)
- Manages resource assignments (accountability)
- Provides safety alarms (safety)
- Records incident event data (reports, training, $$$)

Table 1: Typical Asset Data Available via RSNs

Data	Definition
RSN Presence	RSN detects and reports it is in range of an appropriate Gateway Controller.
RSN Movement	RSN detects and reports that it has begun to move, stopped moving, or has not moved (depending on the application) for some period of time that is configurable.
RSN Shock	RSN detects and reports a mechanical shock that exceeds a preset threshold.
RSN Battery	RSN measures and reports voltage of its internal battery.

Data	Definition
Level	

Note: The movement and shock features can be enabled or disabled by the system. Different "behaviors" can be set for different RSN status or work assignment settings.

5.4 Maintenance Philosophy

This manual supports operational, intermediate and depot levels of maintenance. See below for an abbreviated explanation of each level of maintenance.

Operational This level of maintenance includes all preventive and corrective maintenance that an end user or customer could perform. Performance of this level of maintenance requires no special tools or test equipment.

Intermediate This level of maintenance can only be performed by specially trained, TeraHop certified technicians. This maintenance is typically limited to circuit card assembly replacement, computer assisted setup and calibration of a recently installed network prior to commissioning.

Depot This level of maintenance shall always be performed at a remote site. It will likely be performed at the manufacturing facility or any TeraHop-approved facility. Depot location will also be the site for failed equipment disposition.

5.5 Safety Introduction

This section serves as a single location where the reader can locate the safety admonishments that are applicable to the content contained in this document. Keep in mind that every admonishment contained in this section is a duplicate of an admonishment that is located immediately before the task or procedural step that poses the potential hazard.

5.5.1 Use of Safety Terms

This section explains the difference between DANGERS, WARNINGS, CAUTIONS and Notes. It also explains the structure of the various types of admonishments.

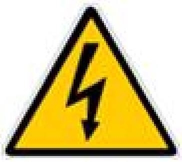
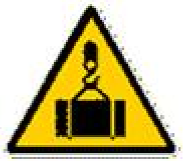
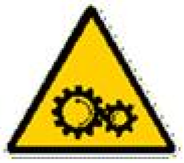
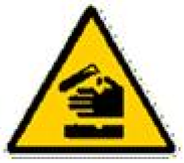
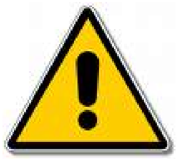
Table 2: Types of Admonishments

Admonishment Category	Description
DANGER	DANGER refers to a situation hazardous to personnel if the information in the DANGER is not observed. Likely consequences are severe injury or death.
WARNING	WARNING refers to a situation hazardous to personnel if the information in the WARNING is not observed. Possible consequences are severe injury or death.
CAUTION	CAUTION refers to a situation in which equipment may be damaged if the CAUTION is not observed.
Note	Note highlights critical information about a procedure or description. A Note does not describe hazards to personnel, equipment or service.

5.5.2 Examples of Caution, Warning, and Danger Icons

These admonishments are represented by a specific icon which corresponds to the type of hazard being advised against. Below are some examples of these icons that are used throughout this manual.

Table 3: Admonishment Icons

Admonishment	Graphic Symbol	Meaning
DANGER/WARNING		Electrical hazard
DANGER/WARNING		Lifting object hazard
DANGER/WARNING		Mechanical hazard
DANGER/WARNING		Chemical hazard
CAUTION		Possible damage to equipment
Note	**Note:**	Highlights critical information. No personnel or equipment hazards.

5.6 General Safety Guidelines

This section lists general admonishments that pertain to electrical equipment. They do not apply to any specific procedure or piece of equipment discussed in this manual. They do apply in general to any/all electrical work. Additionally, this section describes how all admonishments are structured throughout this manual. All admonishments appear immediately before the step or action that poses a potential danger to either personnel or equipment.

As mentioned earlier, Cautions apply to equipment damage or degradation, while Warnings and Dangers apply to personal injury. Warnings indicate a potential for personal injury or even death, while Dangers indicate that the potential for injury or death is very likely, in fact it is a near certainty if the admonishment is not complied with.

All three admonishments are structured in three parts. The first part states the hazard, such as, personal injury, equipment damage, electrical hazard, etc., and explains the hazard in general detail, such as laser light can damage your eyes. The second part explains how to safely work around the hazard; for example, always remove jewelry when working on a live circuit. And the third part states the likely consequences of not following the instructions in the admonishment, such as failure to adhere to this admonishment may result in serious injury or even death. An example of this admonishment is illustrated below.

WARNING

Electrical Hazard

Power connections will be made during this installation that will require the technician to make electrical connections. A simple 12 VDC circuit can be very hazardous.

Make sure all electrical circuits are deenergized to the maximum extent possible. NEVER wear jewelry when working on equipment. NEVER work alone.

Failure to adhere to this warning could result in serious injury or even death.

WARNING

Possible Eye Injury

Drilling holes in a solid surface, metal wood, etc., can result in debris breaking away and traveling at high velocities. This debris can strike an unprotected eye and result in lasting damage.

Always wear protective goggles or eye glasses when drilling.

Failure to adhere to this warning could result in eye injuries that lead to permanent disability, even blindness.

5.7 System-Specific Safety Guidelines

All of the safety admonishments that pertain to this specific piece of equipment are included in this section.

WARNING ⚠

Electrical Hazard

Power connections will be made during this installation that will require the technician to make electrical connections. A simple 12 VDC circuit can be very hazardous.

Make sure all electrical circuits are deenergized to the maximum extent possible. NEVER wear jewelry when working on equipment. NEVER work alone.

Failure to adhere to this warning could result in serious injury or even death.

WARNING

Possible Eye Injury

Drilling holes in a solid surface, metal wood, etc., can result in debris breaking away and traveling at high velocities. This debris can strike an unprotected eye and result in lasting damage.

Always wear protective goggles or eye glasses when drilling.

Failure to adhere to this warning could result in eye injuries that lead to permanent disability, even blindness.

5.8 Unpacking Equipment

The equipment will, in most cases, be delivered by TeraHop Networks Field Support personnel or by TeraHop Networks Channel Partner. In these instances, these individuals will unpack, inventory and explain each piece of equipment to you. The equipment will be provided in the form of a “sales kit” which will include the IMS equipment required along with custom installation hardware that will allow for the professional mounting and or installation of the supplied equipment in the incident command vehicle.

After the unpacking and inventory are complete, the installation process shall begin. Use your applicable sales order during the performance of your equipment inventory. Due to distinctions between each customer, your actual equipment list will be somewhat different.

5.9 Installation Procedure Overview

The hardware installation procedure is divided into several steps:

- Pre-installation vehicle survey
- Mechanical placement and mounting
- Power distribution and power wiring
- Ethernet LAN wiring and installation
- RF / Antenna installation and wiring
- System test and checkout

Refer to each section for installation instructions.

5.10 Pre-Installation Vehicle and Site Survey Forms

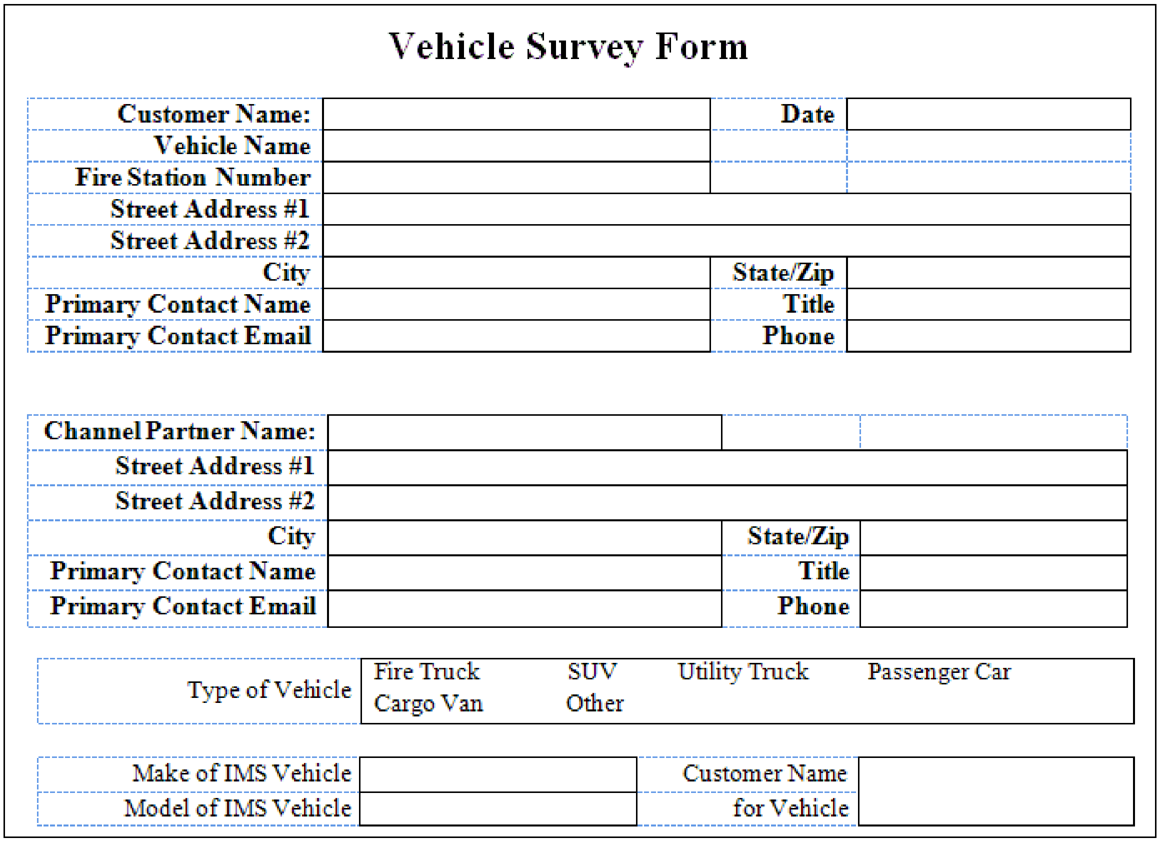
Before installing the system at the customer site, it is important that you understand the vehicles and site where the system is to be installed. To understand the customer's needs, you need to complete the four forms listed below. This survey is available as a MS Word document and is available for download from the TeraHop Customer Resource Management (CRM) tool. For information on accessing the CRM, go to Warranty Service and Technical Support.

The completed survey will identify the vehicles on which the system will be installed, the total number of system components such as MGS, RSNs, PDAs, and Administration Station computer(s) that will be sold to this customer and which will require installation.

The surveys also include questions for you to answer that will help you identify any special needs for the installation. For example, are there any known operational problems with the vehicle? Does the vehicle have an active two-battery configuration or only one active battery?

- Vehicle Survey Form – use this form for each vehicle at the site to identify its make/model and any specific installation needs.
- IMS Component Quantities per Site – use this form is to capture all necessary data on the type and quantity of components ordered for a particular site.
- IMS Component Quantities per Vehicle – use this form is to capture all necessary data regarding the type and quantity of components ordered for a particular vehicle.
- Fixed Site Survey Form – use this form to capture all necessary data about the site, such as facility, user area, the RF environment for the 5 GHz and 2.4 GHz bands, and preliminary access points.

5.10.1 Vehicle Survey Form



Vehicle Survey Form

Customer Name:		Date	
Vehicle Name			
Fire Station Number			
Street Address #1			
Street Address #2			
City		State/Zip	
Primary Contact Name		Title	
Primary Contact Email		Phone	

Channel Partner Name:			
Street Address #1			
Street Address #2			
City		State/Zip	
Primary Contact Name		Title	
Primary Contact Email		Phone	

Type of Vehicle	Fire Truck SUV Utility Truck Passenger Car Cargo Van Other

Make of IMS Vehicle		Customer Name for Vehicle	
Model of IMS Vehicle			

Special Notes / Concerns:

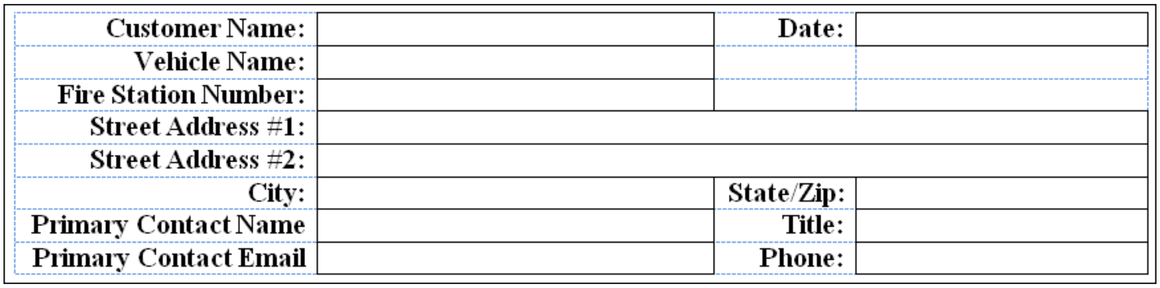
1. Are there any known operational problems with the vehicle?
2. What are the customer's installation constraints? (e.g. drilling holes)
3. Are there any special customized aesthetic requirements?
4. Where will the Gateway Router be installed on the exterior of the vehicle?
5. Where is the available space for the rack in the vehicle for installation of the IMS components? (some empty areas may be for a purpose)
6. Are there other mountings or antenna systems currently on the vehicle?
7. If so, are we able to use the existing conduits to run our cables?
8. Are there any other systems being powered directly from the vehicle battery?
9. If so, are we able to follow the same path to run our vehicle power cables?
10. Does the vehicle have an active two battery configuration or only one active battery?

11. If so, is the primary battery properly charging the secondary battery?
12. What is the distance in feet from the vehicle battery to the proposed location of the equipment? (the length determines the wire gauge used)
13. If possible gather the technical data for the batteries in the vehicle. (make, power rating, age)
14. If possible run a test on each battery to determine the health of the battery.
15. Using a voltmeter, verify that the input voltage to the Inverter is greater than 11VDC and less than 15VDC. If not, the vehicle battery must be replaced with another that provides the designated amount of voltage. If the battery is not replaced the system may incur damage or not function properly.
16. Determine how large of an inline surge protector or fuse needs to be installed to protect against power surges that could damage the IMS system.

5.10.2 IMS Component Quantities per Vehicle Form

Incident Management System (IMS) Component Quantities per Vehicle

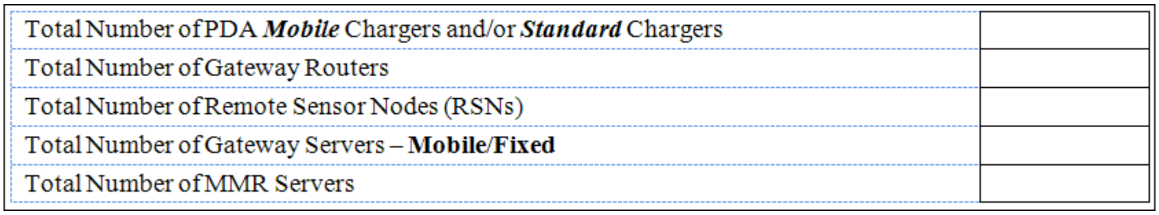
The purpose of this form is to capture all necessary data regarding the type and quantity of components ordered for a particular vehicle.



Customer Name:		**Date:**	
Vehicle Name:			
Fire Station Number:			
Street Address #1:			
Street Address #2:			
City:		**State/Zip:**	
Primary Contact Name		**Title:**	
Primary Contact Email		**Phone:**	

The recommended places for various components are as follows:

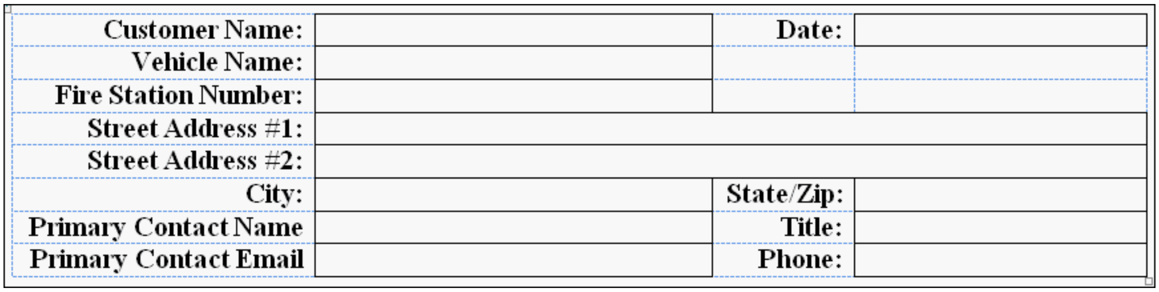
Vehicle: 1st Gateway Router, Gateway Server, MMR System, Ethernet Switch, 2 PDAs, 1st Mobile PDA Charger, Inverter, and a mounted RSN in the front and rear of each vehicle.



Total Number of PDA ***Mobile*** Chargers and/or ***Standard*** Chargers	
Total Number of Gateway Routers	
Total Number of Remote Sensor Nodes (RSNs)	
Total Number of Gateway Servers – **Mobile/Fixed**	
Total Number of MMR Servers	

5.10.3 Incident Management System (IMS) Component Quantities per Site

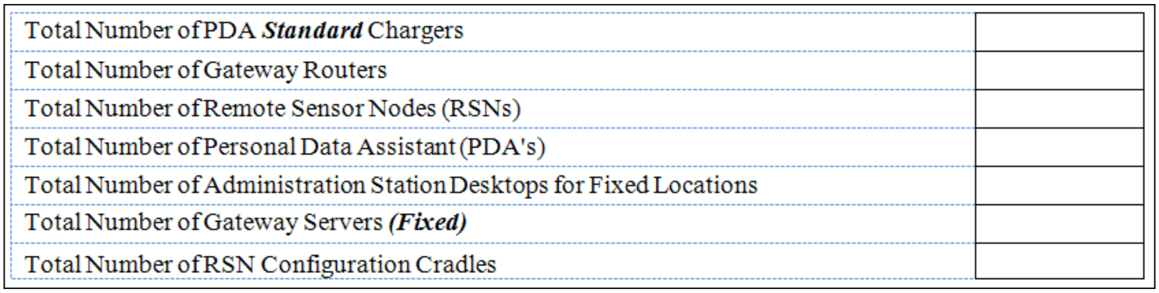
The purpose of this form is to capture all necessary data on the type and quantity of components ordered for a particular site or vehicle.



Customer Name:		**Date:**	
Vehicle Name:			
Fire Station Number:			
Street Address #1:			
Street Address #2:			
City:		**State/Zip:**	
Primary Contact Name		**Title:**	
Primary Contact Email		**Phone:**	

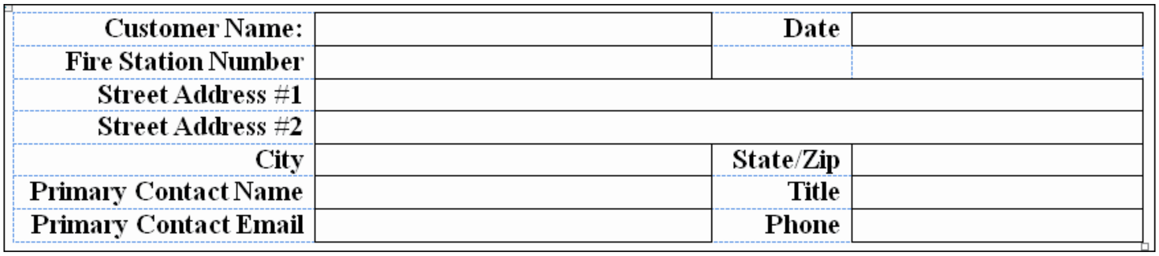
Fixed Location: 2nd Gateway Router, 2nd Mobile PDA Charger, And Standard Desktop Charger for PDA, RSN Configuration Cradles, and the Administration Station PC. The Administration Station needs to be housed in the same Fire Station as the vehicle that the IMS System is installed in. Both the RCT and the ADM Station located in close proximity will facilitate Wi-Fi “Merging” of the Gateway Routers. In addition, the incident logs generated during system use will be extracted to the Administration Station. Else, the vehicle will have to be driven to where the fixed Administration Station and fixed Gateway Router are located to have the data download performed.

The RSN Configuration Cradle should be located with the PC and used by whoever will be using the RSN Configuration Tool application (RCT). Ideally, the System Administrator will work a standard business work week. If not, there needs to be a designated IMS System and RSN Administrator per shift.



Total Number of PDA ***Standard*** Chargers	
Total Number of Gateway Routers	
Total Number of Remote Sensor Nodes (RSNs)	
Total Number of Personal Data Assistant (PDA's)	
Total Number of Administration Station Desktops for Fixed Locations	
Total Number of Gateway Servers ***(Fixed)***	
Total Number of RSN Configuration Cradles	

5.10.4 Fixed Site Survey Form



Customer Name:		**Date**	
Fire Station Number			
Street Address #1			
Street Address #2			
City		**State/Zip**	
Primary Contact Name		**Title**	
Primary Contact Email		**Phone**	

1. Obtain a facility diagram. Before getting too far with the site survey, locate a set of building blueprints. If none are available, prepare a floor plan drawing that depicts the location of walls, walkways, etc.
2. Visually inspect the facility. Be sure to walk through the facility before performing any tests to verify the accuracy of the facility diagram. This is a good time to note any potential barriers that may affect the propagation of RF signals. For example, a visual inspection will uncover obstacles to RF such as metal racks and partitions, items that blueprints generally don't show.
3. Identify user areas. On the facility diagram, mark the areas of where fixed IMS system components are proposed to be located.
4. Perform an RF Survey for the 5 GHz and 2.4 GHz bands. This would warrant the use of a spectrum analyzer or a smaller handheld wireless Wi-Fi finder (such as a ZyXEL AG-225H) to characterize the interference, especially if there are no other indications of its source. Based on the results of the testing, you might need to reconsider the location of some access points and redo the affected tests.
5. Determine preliminary access point locations. By considering the location of wireless users and range estimations of the wireless LAN products you're using, approximate the locations of access points that will provide adequate coverage throughout the user areas. Plan for some propagation overlap among adjacent access points, but keep in mind that channel assignments for access points will need to be far enough apart to avoid inter-access point interference.

   Be certain to consider mounting locations, which could be vertical posts or metal supports above ceiling tiles. Be sure to recognize suitable locations for installing the access point, antenna, data cable, and power line. Also think about different antenna types when deciding where to position access points. An access point mounted near an outside wall, for example, could be a good location if you use a relatively high gain oriented within the facility.
6. Verify access point locations.

   Install an access point at each preliminary location, and monitor the site survey software readings by walking varying distances away from the access point. There's no need to connect the access point to the distribution system because the tests merely ping the access point; however, you'll need AC power. So be sure to take along an extension cord, and learn where AC outlets exist.

   Take note of data rates and signal readings at different points as you move to the outer bounds of the access point coverage. In a multi-floor facility, perform tests on the floor above and below the access point. Keep in mind that a poor signal quality reading likely indicates that RF interference is affecting the wireless LAN.

7. Document findings. Once you're satisfied that the planned location of access points will provide adequate coverage, identify on the facility diagrams recommended mounting locations. Of course the installers will need this information.

5.11 Mechanical Placement and Mounting

Locate each piece of equipment. Use the following paragraphs to mount the equipment.

5.11.1 THN Gateway Router

Figure 8: THN Gateway Router

WARNING

Possible Eye Injury

Drilling holes in a solid surface, metal wood, etc. can result in debris breaking away and traveling at high velocities. This debris can strike an unprotected eye and result in lasting damage.

Always wear protective goggles or eye glasses when drilling.

Failure to adhere to this warning could result in eye injuries that lead to permanent disability, even blindness.

This unit is normally mounted to the roof of the vehicle to provide external coverage to the RSNs. In most installations, the router will mount to a pole via a back plate bracket. The bottom of the pole fits within an elbow with a friction lock knob to hold the pole in a lowered or raised position (see the illustration below of a mast pin). Any mounting hardware and vehicle holes must be sufficiently weatherproof to prevent leakage.

5.11.2 Gateway Server

The Gateway Server is a Linux-based mobile PC. It is rated for automotive use, however it is not weatherproof. It must be mounted within the vehicle. Use specific hardware appropriate for the particular installation requirements. Typically, 5/16 x 24 screws should be used to mount the unit. Since this unit requires forced air ventilation, leave space around the unit to facilitate proper cooling.

5.11.3 MMR System

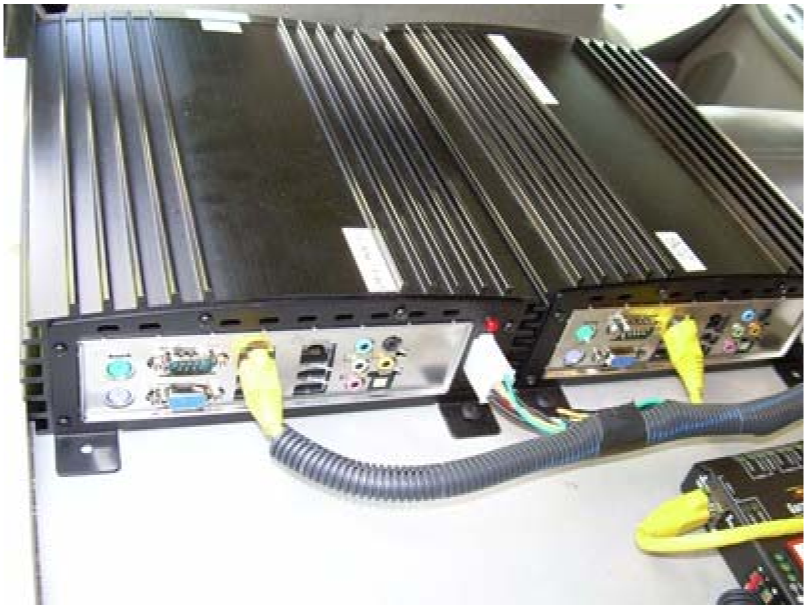


Figure 9: MMR System and Gateway Server

The MMR System is a Windows-based mobile PC. It is rated for automotive use, however it is not weatherproof. It must be mounted within the vehicle. Use specific hardware appropriate for the particular installation requirements. Typically, 5/16 x 24 screws should be used to mount the unit. Since this unit requires forced air ventilation, leave space around the unit to facilitate proper cooling.

5.12 Power Distribution

Warning

Electrical Shock Hazard

Power connections will be made during this installation that will require the technician to make electrical connections. A simple 12 VDC circuit can be very hazardous.

Make sure all electrical circuits are deenergized to the maximum extent possible. NEVER wear jewelry when working on equipment. NEVER work alone.

Failure to adhere to this warning could result in serious injury or even death.

Proper power distribution is critical for reliable system operation. The following sections define the requirements and procedure for installation and wiring of the power distribution components.

5.12.1 Unit Power Requirements

The worst-case power requirements of each component are listed in the table below:

Table 1. Unit Power Requirements

Component	Nominal Voltage	Max. Wattage / Current
THN Gateway Router	12VDC (11.8 → 14 VDC)	2.2A (negative ground only)
Gateway Server Linux PC	12VDC (11.8 → 14 VDC)	2.7A (negative ground only)
MMR System Windows PC	12VDC (11.8 → 14 VDC)	2.7A (negative ground only)
Garrett Ethernet Switch	12VDC (11.8 → 14 VDC)	0.25A (negative ground only)

Note: This equipment will not work in positive ground vehicles.

5.12.2 Total System Power Requirements

Based on the unit power requirements listed above, the overall system power requirements can be calculated as follows:

Total Power required for 12V components: 94.2W (7.85A@ 12VDC)

5.12.3 Power Distribution Installation

Warning

Electrical Shock Hazard

Power connections will be made during this installation that will require the technician to make electrical connections. A simple 12 VDC circuit can be very hazardous.

Make sure all electrical circuits are deenergized to the maximum extent possible. NEVER wear jewelry when working on equipment. NEVER work alone.

Failure to adhere to this warning could result in serious injury or even death.

Using the Power Distribution diagram on the next page**,** confirm that all system components have been properly mounted, wire the system based on the procedure listed on the pages following the diagram.

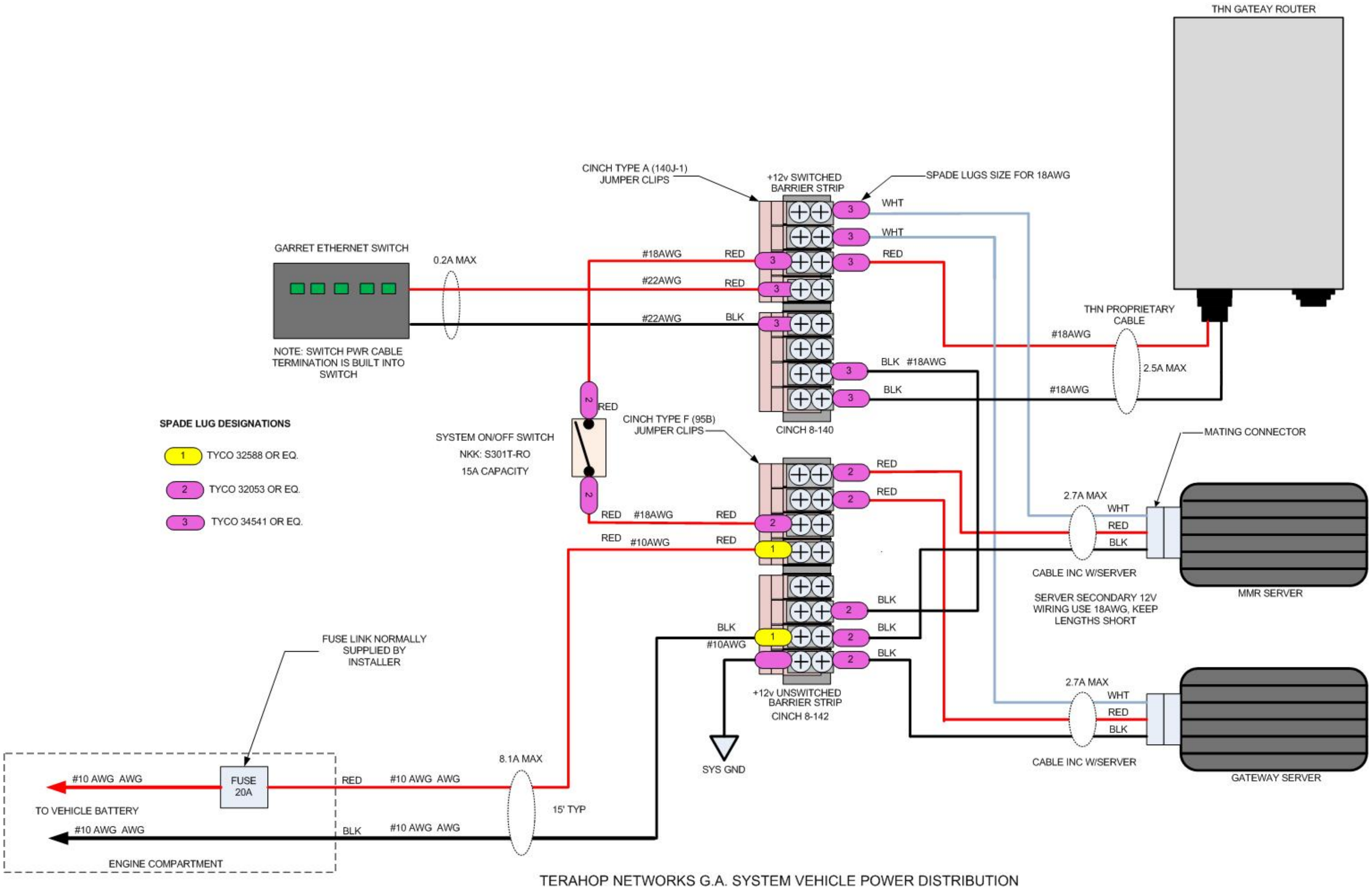


Figure 10: TeraHop Networks System Vehicle Power Distribution Diagram

5.12.4 System Power Switch

The system power switch is a heavy duty toggle switch with a rating of 15A at 12VDC. This provides a safety factor of approximately 50%. Mount the switch in a convenient location, since it is used as the primary system power switch.

Wire the system power switch as shown in the power distribution diagram.

5.12.4.1 Barrier Strip Wiring

Two barrier strips are used, as shown in the diagram: switched and un-switched. The un-switched barrier strip is used to provide constant power to the mobile PCs, and to provide a convenient connection point for any connected equipment that should operate in the un-switched mode. The switched barrier strip is used to connect to the “ignition” wires of the server PCs so they shut down gracefully (delayed) when switched off. This prevents file corruption. The Gateway Router (GR), and Ethernet switch also connect to switched power.

The system power toggle switch connects the barrier strips together, and provides switched power to the switched barrier strip.

Connect all equipment to the switched barrier strip except the main power leads of the mobile PCs (servers).

Note: Items of equivalent current carrying capacity such as ring lugs, spade lugs, barrier strips, or barrier jumpers may be used.

5.12.4.2 Gateway Server

Use the following procedure to install the power wiring to the Gateway Server:

1. Locate the preformed mobile PC cable harness.
   Note: It uses the 8-conductor Molex connector to plug into the PC. Since this harness is only about 12 inches long, it may be necessary to extend the red, black, and white power wires to reach the barrier strips. It is acceptable to use butt splices to extend the power wires. Make sure any wire used to extend is a minimum of 18AWG.
2. Connect (via crimp spade lugs) the power wires to the distribution strips as shown in the power distribution diagram.
3. Dress and tape the remainder of the wires in the harness, since they are unused.

5.12.4.3 MMR System

Use the following procedure to install the power wiring to the Gateway Server:

1. Locate the preformed mobile PC cable harness.
   Note: It uses the 8-conductor Molex connector to plug into the PC. Since this harness is only about 12" long, it may be necessary to extend the red, black, and white power wires to reach the barrier strips. It is acceptable to use butt splices to extend the power wires. Make sure any wire used to extend is minimum of 18AWG.
2. Connect (via crimp spade lugs) the power wires to the distribution strips as shown in the power distribution diagram.
3. Dress and tape the remainder of the wires in the harness, since they are unused.

5.12.4.4 TeraHop Network Gateway Router

1. Locate the Gateway Router (GR) power harness supplied with the GR unit.
2. Connect the weatherproof connector to the power input on the GR unit.
3. Connect the other end to the power distribution barrier strip, using the appropriate spade lug, sized for 18AWG wire.

5.12.4.5 Garrett Ethernet Switch

1. Connect a 22 AWG red jumper wire from the positive input block on the Ethernet switch to the positive side of the distribution barrier strip.
2. Connect a 22 AWG black jumper wire from the negative input block on the Ethernet switch to the negative side of the switched distribution barrier strip.
   Note: Heavier gauge wire may be used if 22AWG wire is unavailable.

5.12.5 LAN Ethernet Cabling

Refer to the following diagram to connect the Ethernet cables to the various system components. Locate the Garrett Ethernet switch, since all LAN cables are routed from the respective components to the switch. See the Ethernet Network Wiring Diagram below.

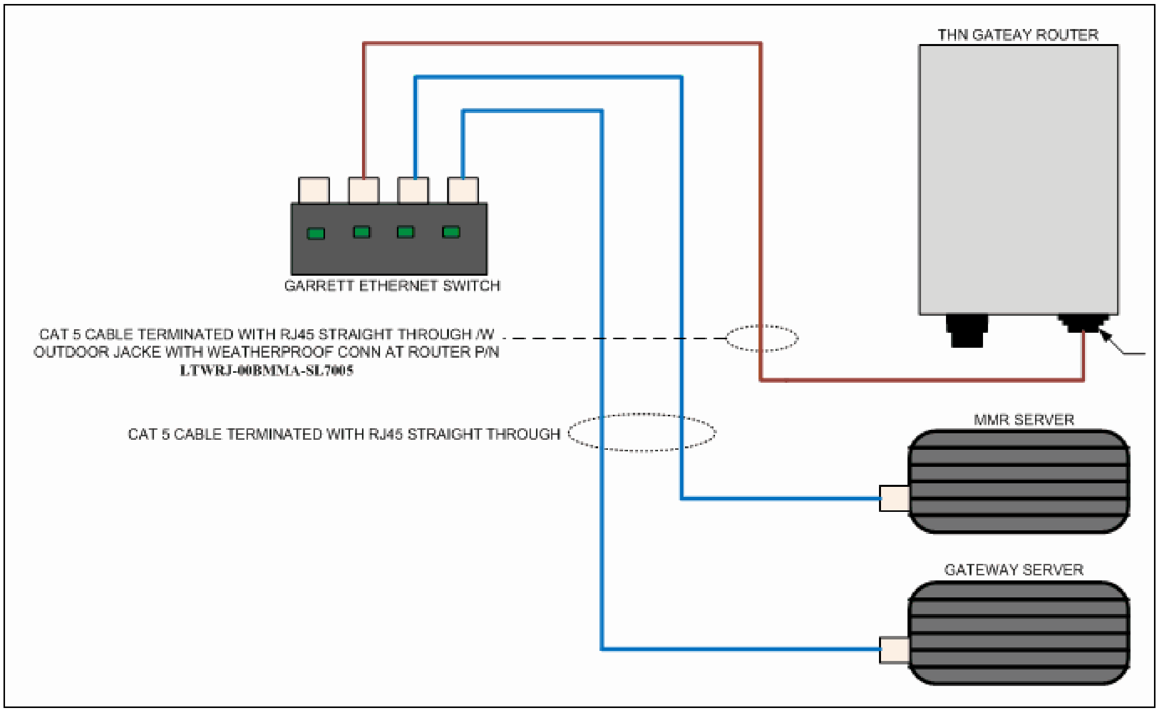

THN GATEAY ROUTER
GARRETT ETHERNET SWITCH
CAT 5 CABLE TERMINATED WITH RJ45 STRAIGHT THROUGH /W OUTDOOR JACKE WITH WEATHERPROOF CONN AT ROUTER P/N LTWRJ-00BMMA-SL7005
CAT 5 CABLE TERMINATED WITH RJ45 STRAIGHT THROUGH
MMR SERVER
GATEWAY SERVER

Figure 11: TeraHop Networks Ethernet Network Cabling

Since the Ethernet Switch has MDIX capable ports, crossover cables are not required. Use straight through cables for all connections. When determining length, leave adequate extra length to account for future relocation or connector repair.

1. Locate the Gateway Server mobile PC. Connect a CAT-5 RJ45 terminated cable from the server Ethernet jack to a port on the Ethernet switch.
   Note: the specific port used is not critical. All ports are equivalent from a connection viewpoint.
2. Locate the MMR System mobile PC. Connect a CAT-5 RJ45 terminated cable from the server Ethernet jack to a port on the Ethernet switch.
   Note: the specific port used is not critical. All ports are equivalent from a connection viewpoint.
3. Locate the THN Gateway Router. This unit is normally located on the roof of the vehicle on a retractable mast. The outdoor rated Ethernet cable that is provided is equipped with the correct weatherproof boot for the router end of the cable. Make sure the boot is properly secured to the GR's connector.

4. To facilitate installation through the vehicle roof, the switch end of the supplied GR Ethernet cable is not terminated. This cable must be terminated into a standard compatible RJ45 connector using an industry standard crimp tool.
5. Using a vacant port, connect the other end of the cable to the Ethernet switch.

6.0 Software Installation and Update

6.1 Software Installation and Configuration

6.1.1 Introduction

All system software is pre-loaded (see System Software Overview). You will, however, need to configure the following components:

- The Administration Station (ADMS) Wi-Fi connection is configured for the IMS. See Setting the Administration Station (ADMS) SSID to Connect to the Mobile Gateway System (MGS).
- The IMS Personal Digital Assistant (PDA) needs to be configured for the customer. You configure the PDA using the IMS Application Configuration Tool (ACT) which resides on the ADMS laptop computer. See Configuring the IMS Application.
- The Remote Sensor Nodes (RSNs) need to be set up with configurations. You create configurations and download them to RSNs using the RSN Configuration Tool (RCT) which resides on the TeraHop Console in the ADMS laptop computer. See Configuring RSNs.
- The CustomerID and First Responder bit are configured in the MMR. See How to Edit CustomerID and AcceptFirstResponder Options in the MMR.
- Once the hardware is set up and the PDAs and RSNs have been configured, the entire system needs to be tested and checked out. See Operational Checkout and System Commissioning.

6.1.2 Intended Audience

This section is intended to outline the procedure to update the TeraHop Incident Management System (IMS). It assumes the components are, at a minimum, loaded with the factory base software image, the MMR pre-registered at TeraHop, and that the 4-digit Area ID is known.

6.2 System Software Overview

The TeraHop Incident Management System with Automated Accountability (IMS) contains the following software components:

Remote Sensor Node (RSN) pre-loaded with

- TeraHop Operating System
- TeraHop Networks RSN Firmware

Gateway Router pre-loaded with

- Linux Operating System
- TeraHop Operating System
- TeraHop Networks GR Application

Gateway Server pre-loaded with

- Linux Fedora 10 Operating System
- TeraHop Networks GS Software

Ethernet Switch (no software)

Message Management and Routing (MMR) System pre-loaded with

- Microsoft Windows Server 2003 Operating System
- TeraHop Networks MMR Software
- TeraHop Networks IMS Application

Personal Digital Assistant (PDA) pre-loaded with

- Windows Mobile 5.0 Operating System
- TeraHop IMS Client Application
- Open NetCF
- Windows Compact Framework 2.0, 3.5

IMS Software Components (continued on next page)

IMS Software Components (continued)

Administration Station (ADMS) Laptop Computer pre-loaded with

- Microsoft Windows XP Professional Operating System
- TeraHop Console (THC) Software
- Application Configuration Tool (ACT)
- Required THC ADD-Ins:
  - Incident Log Data Transfer Tool (TDX)
  - RSN Configuration Tool (RCT)
  - RSN Configuration Viewer (RCV)
  - ADMS-MMR Data Services

RSN Configuration Tool (RCT) Cradle does not contain any software. The software that runs it resides on other host machines.

6.2.1 Re-Installing Software

If you should need to re-install the software on any of these components, contact TeraHop Customer Service by e-mail or call 770-663-3455.

6.2.2 Updating Software

When an update to any of the system components becomes available, TeraHop Networks Customer Service will contact you. The update, as well as detailed update instructions, will be made available through the TeraHop Networks Customer Resource Management (CRM) System.

6.3 How to Edit CustomerID and AcceptFirstResponder Options in the MMR

The Message Management and Routing (MMR) System is shipped from the factory with a default CustomerID of 70. When setting up the IMS for a customer, you must change the default CustomerID in the MMR to the CustomerID that TeraHop Networks assigns for the purchased IMS. TeraHop Networks provides the assigned CustomerID in the shipping papers sent with the system.

The MMR Configuration Editor is a software tool used to edit the CustomerID and AcceptFirstResponders options in the MMR. This tool is accessible from the TeraHop Networks Customer Relationship Management (CRM) System available through the Internet to authorized users.

Once you obtain the Configuration Editor software, do the following:

1. Connect a VGA monitor, keyboard with PS/2 Connector (USB with PS/2 adapter acceptable), and a mouse with PS/2 connector (USB with PS/2 adapter acceptable) to the MMR.

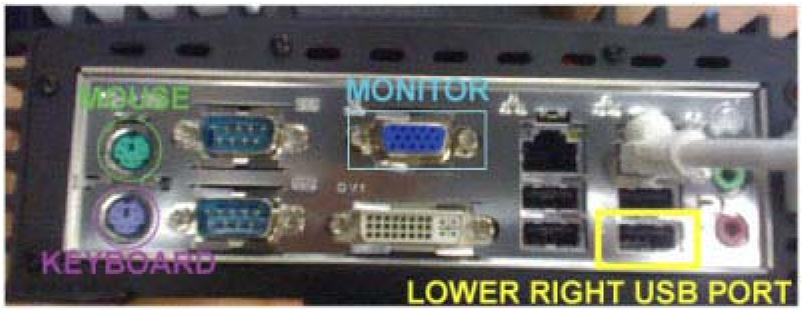
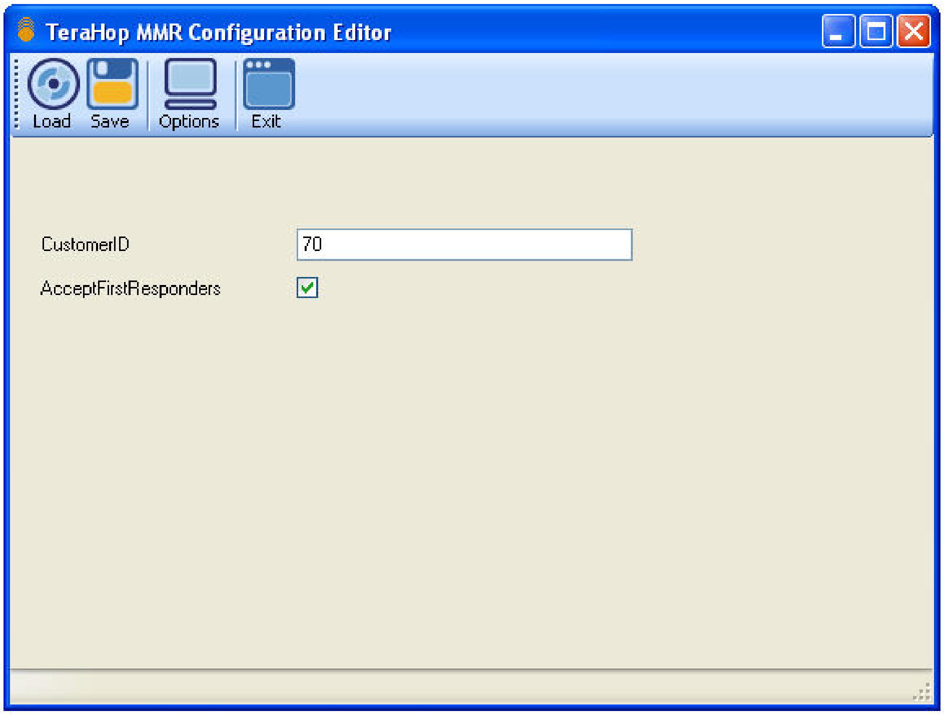


Figure 12: Back of ADMS Laptop Computer

2. Copy the MMR Configuration Editor application from the Documents section in the TeraHop CRM to a Flash drive (245 MB or better).
3. Insert the Flash drive into the MMR lower right USB port.
4. Locate the **TeraHop.MMR.Configurator.exe** file on the Flash drive, and double-click to execute.
   When executed, the MMR Configuration Editor automatically displays the **CustomerID** and **AcceptFirstResponders** options from the default location in the MMR. See the illustration below. If you do not see this screen, see **Configuration Files Not Found** on the next page for instructions on how to enter the path name to these options.



CustomerID 70

AcceptFirstResponders ☑

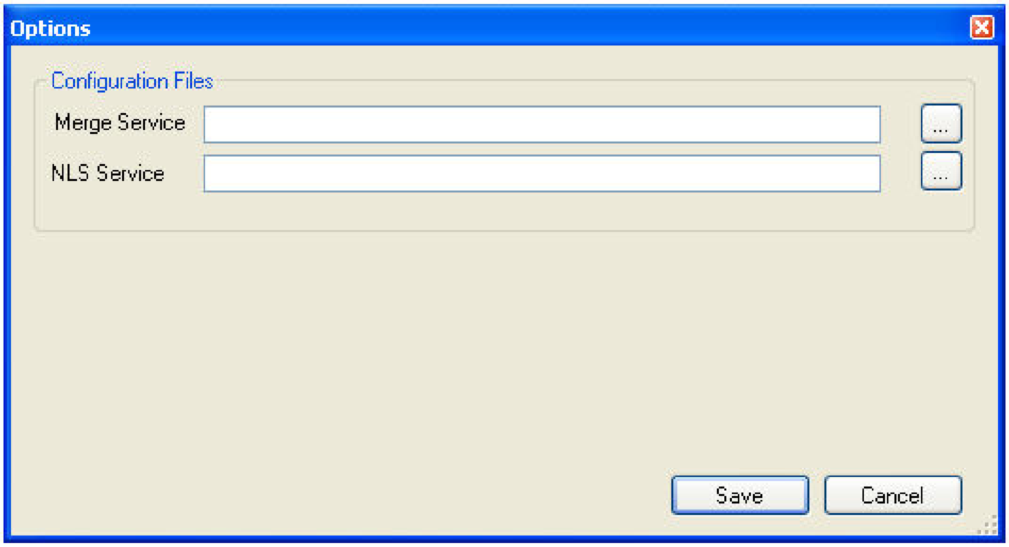
5. In the **CustomerID** field, change the 70 to the CustomerID number that appears in your IMS shipping papers.
6. Set the **AcceptFirstResponders** check box according to the instructions with the TeraHop purchase information.
   This check box ensures that any other First Responders with RSNs (including those from other agencies) will appear on your IMS and can be accepted into an incident. Improper setting will result in undesirable system operation.
7. Click **Save**.
8. Reboot the MMR by turning off the system with the ignition switch. Make sure the MMR completely shuts down before turning it back on.

Configuration Files Not Found

When you insert the Flash drive into the MMR, if the configuration files cannot be found from their default locations (the screen above does not appear), you will see the following message: *The configuration files could not be found. Click on Options to enter the paths for the NLS and Merge configuration files.*

Do the following:

1. Click **Options**.
   The **Options** screen appears.



2. In the **Merge Service** field, enter **C:\Program Files\TeraHop Networks\Merge Service\TeraHop.Services.Merge.exe.config**.
3. In the **NLS Service** field, enter **C:\Program Files\TeraHop Networks\NLS Service\NLSService.exe.config**.
4. Click **Save**.
   The fields should now appear on the screen so that you can enter the new Customer ID.
5. Continue to Step 5 above.

6.4 Setting the Administration Station (ADMS) SSID to Connect to the Mobile Gateway System (MGS)

6.4.1 Determine the SSID

You will be required to configure the ADMS to connect to the correct SSID. To determine the SSID, use the TeraHop Calculator. See How to Use the TeraHop Calculator for Mobile Gateway Systems.

Note: The Access Point SSID is the correct SSID. DO NOT use the Wireless Mesh SSID.

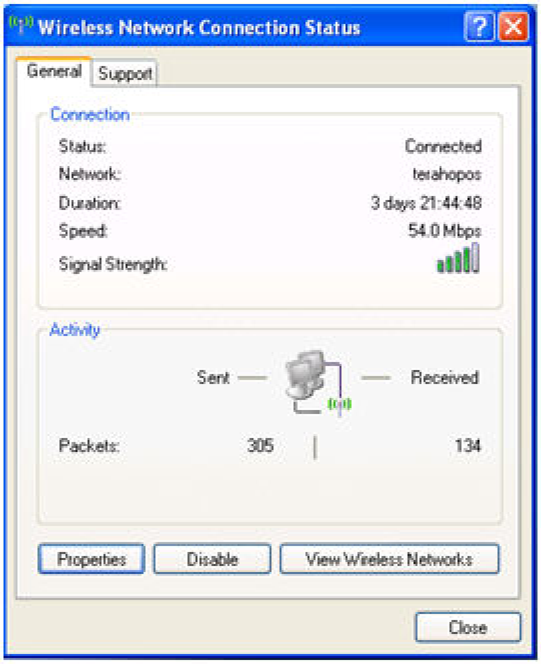
6.4.2 Setting the SSID

1. From the **Start** menu, select **Control Panel**.

   or

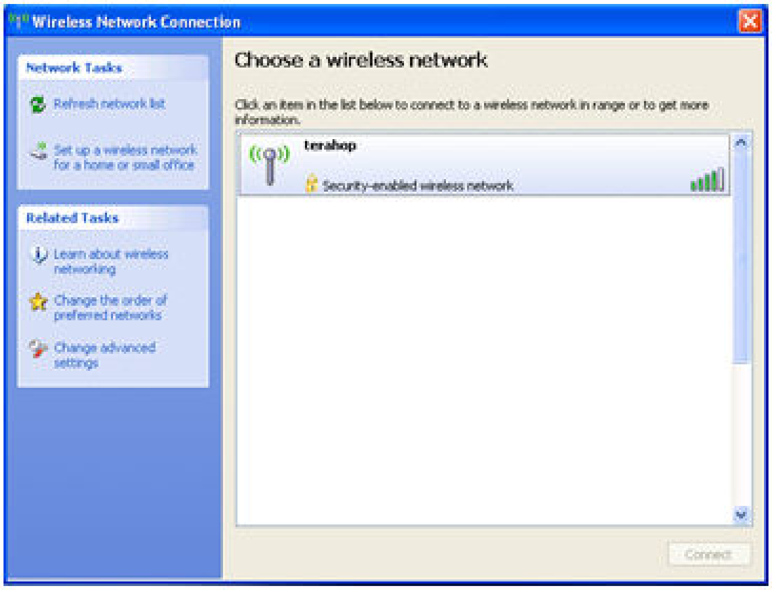
From the **Start** menu, select **Settings**, and then select **Control Panel**.

2. Double-click **Network Connections**.
3. Double-click **Wireless Network Connection**.
4. If the **Wireless Network Connection Status** dialog box opens, click **View Wireless Networks**.



Status: Connected
Network: terahopos
Duration: 3 days 21:44:48
Speed: 54.0 Mbps
Signal Strength:
Packets: 305 | 134

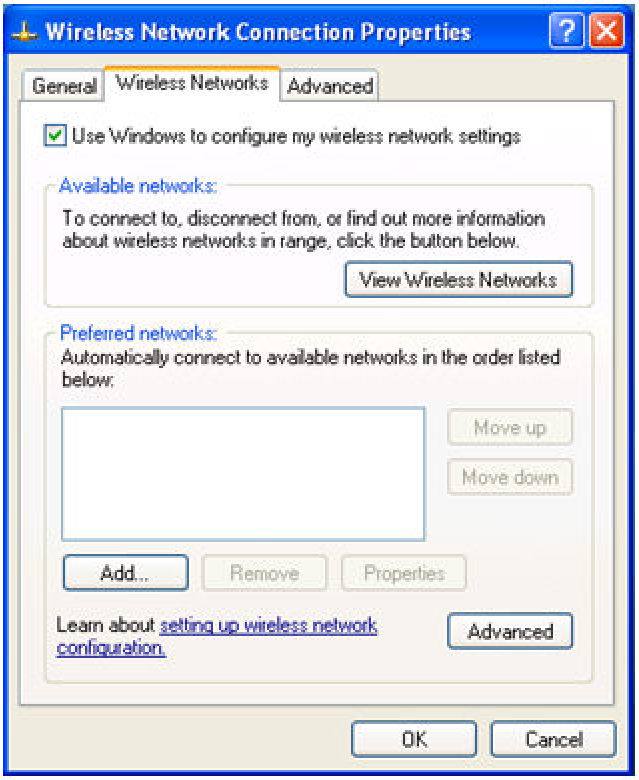
5. Click **Change the order of preferred networks**.


Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Connect

Click an item in the list below to connect to a wireless network in range or to get more information.

terahop
Security-enabled wireless network

6. Check **Use Windows to configure my wireless network settings**.
7. In the **Preferred networks** section, highlight any networks in the list and click **Remove** to clean out the list.
8. In the **Preferred networks** section, click **Add**.



☑ Use Windows to configure my wireless network settings

Available networks:

To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.

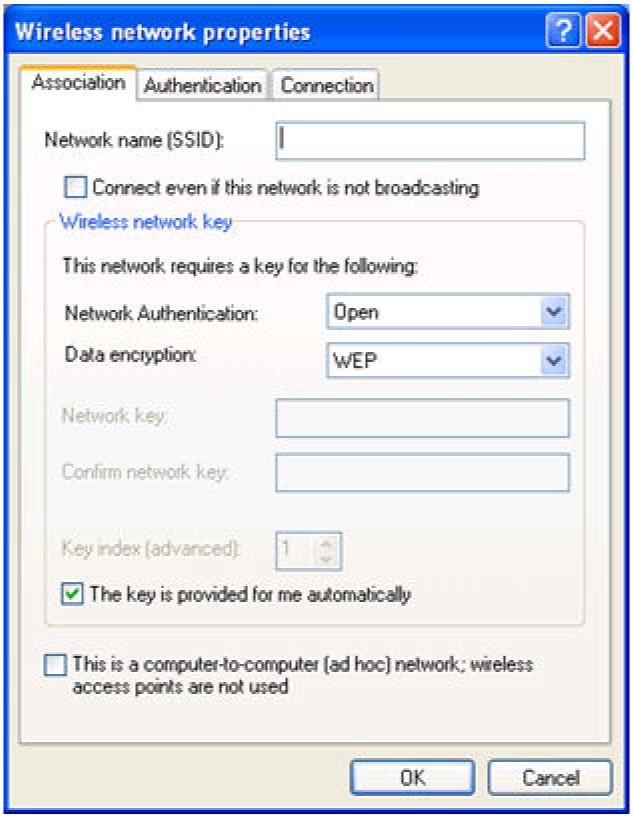
Preferred networks:

Automatically connect to available networks in the order listed below:

Learn about setting up wireless network configuration.

9. Enter the SSID from the previous section.
10. In the Network Authorization field, click the drop-down arrow and select **Open**.
11. In the **Data encryption** field, click the drop-down arrow and select **WEP**.

12. Click to select the **The key is provided to me automatically** check box.



Network name (SSID):

□ Connect even if this network is not broadcasting

Wireless network key

This network requires a key for the following:

Network Authentication: Open

Data encryption: WEP

Network key:

Confirm network key:

Key index (advanced): 1

☑ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

13. Click **OK**.

14. Click **OK** again.

If the MGS is not within range or not running, you may see the following message: *Unable to connect to preferred wireless network.*

Suggested Settings

Below is a list of settings that will optimize performance of the ADMS.

Power Settings

1. Click **Start** (Settings if visible) and select **Control Panel** (performance and maintenance if visible).
2. Select **Power Options**.
3. Set all Plugged-In options to **Never**.
   This will prevent the ADMS from sleeping. If the ADMS is asleep it will not detect the MMR automatically.

SSID

Be sure the only SSID in the Preferred networks list is the SSID of the Gateway Router. If others exist, the ADMS may connect to another SSID and will not connect to the MMR.

Time Zone

Be sure the time zone is properly set. This may interfere with data exchange.

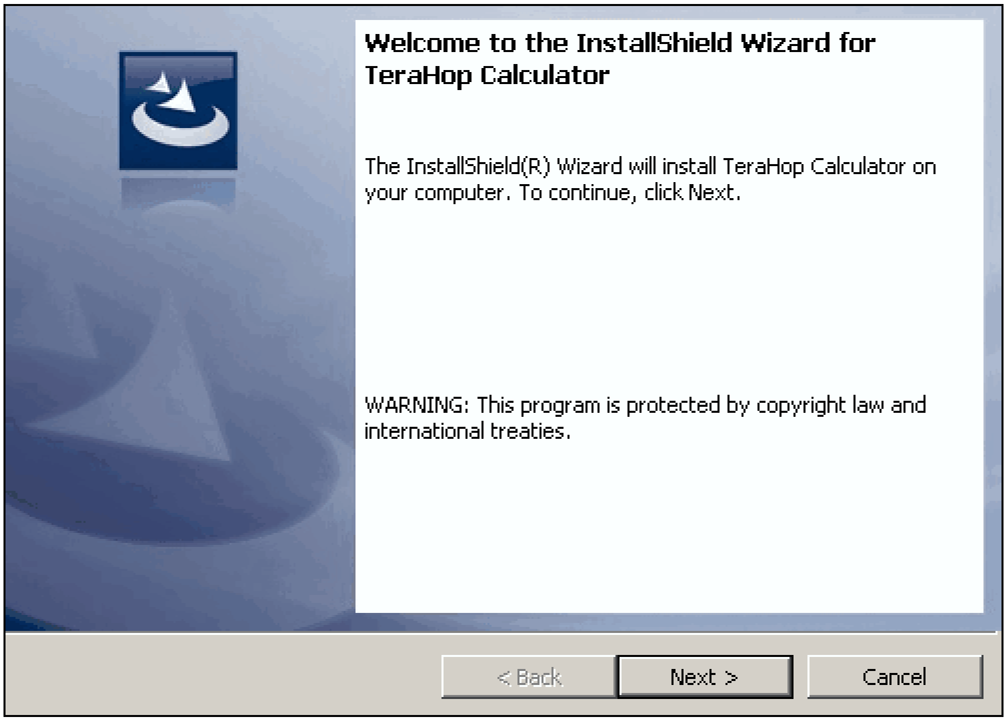
6.5 Installing the TeraHop Calculator for Mobile Gateway Systems (MGS)

The TeraHop Calculator is used to calculate the Gateway Server's IP Address, the Access Point's SSID and the Wireless Mesh's SSID with only the Area ID.

The installation software for this application can be accessed in the TeraHop Customer Relationship Management (CRM) system located on the **Documents** tab under the **Support** drop-down menu.

TeraHop Calculator

1. After downloading the install from the location above, double-click the **msi** file to start the installation.
   The **InstallShield Wizard** screen appears.



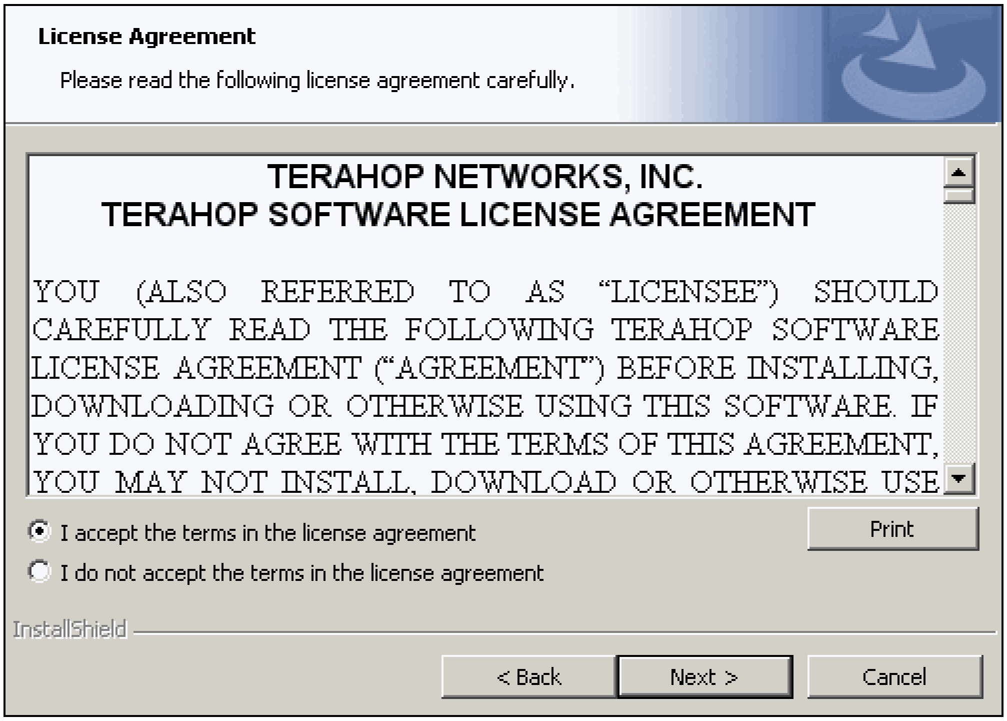
Welcome to the InstallShield Wizard for TeraHop Calculator

The InstallShield(R) Wizard will install TeraHop Calculator on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

2. Click **Next** to continue.

The **License Agreement** screen appears.



License Agreement

Please read the following license agreement carefully.

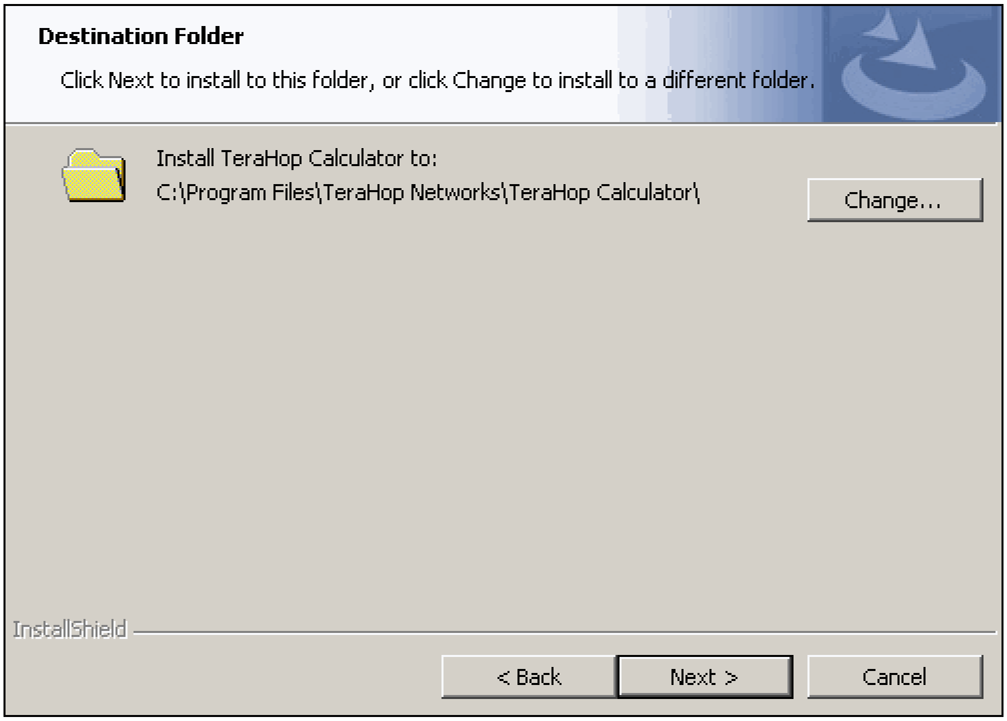
TERAHOP NETWORKS, INC.
TERAHOP SOFTWARE LICENSE AGREEMENT

YOU (ALSO REFERRED TO AS "LICENSEE") SHOULD CAREFULLY READ THE FOLLOWING TERAHOP SOFTWARE LICENSE AGREEMENT ("AGREEMENT") BEFORE INSTALLING, DOWNLOADING OR OTHERWISE USING THIS SOFTWARE. IF YOU DO NOT AGREE WITH THE TERMS OF THIS AGREEMENT, YOU MAY NOT INSTALL, DOWNLOAD OR OTHERWISE USE

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

3. Click the **I accept the terms of the license agreement** radio button, and click **Next** to continue.
   The **Destination Folder** screen appears.

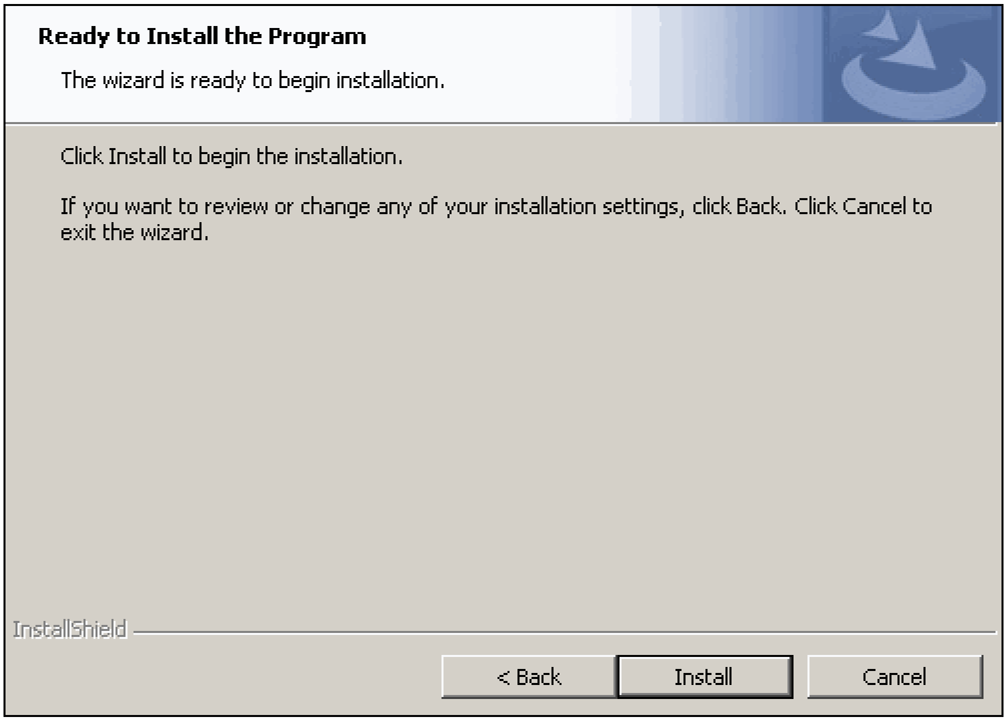


Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install TeraHop Calculator to:
C:\Program Files\TeraHop Networks\TeraHop Calculator\

4. Click **Next** to install the application to the folder on the screen, or click **Change** to install the application to a different folder.
   The **Ready to Install the Program** screen appears.



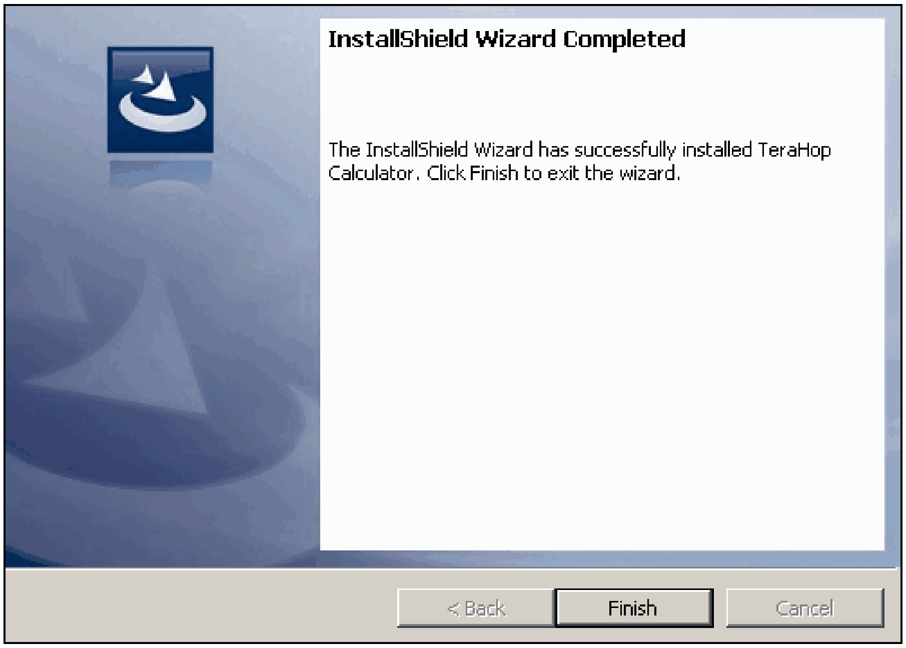
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

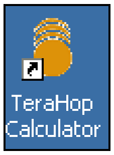
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

5. Click **Install** to begin the installation.
   When the installation is complete, the **InstallShield Wizard Completed** screen appears.



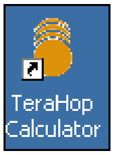
InstallShield Wizard Completed

The InstallShield Wizard has successfully installed TeraHop Calculator. Click Finish to exit the wizard.

6. Click **Finish**.
   The Calculator is installed, and the application shortcut icon appears on the computer desktop. 

7. To begin using the TeraHop Calculator, go to How to Use the TeraHop Calculator for MGS.

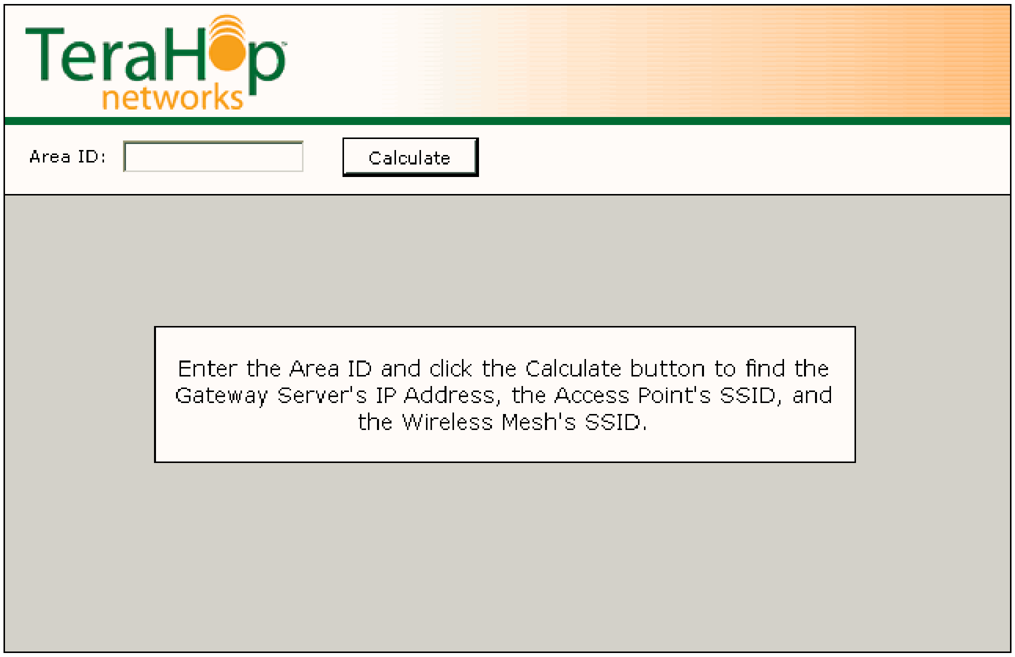
6.6 How to Use the TeraHop Calculator for Mobile Gateway Systems



The TeraHop Calculator for Multiple Gateway Systems (MGS) is used to calculate the Gateway Server’s IP Address, the Access Point’s SSID and the Wireless Mesh’s SSID by entering only the Area ID. The Area ID is found on the label on the Gateway Router.

To run the TeraHop Calculator for MGS, do the following:

1. On the computer desktop, click the **TeraHop Calculator** Icon to start the application. The **Area ID entry** screen appears.

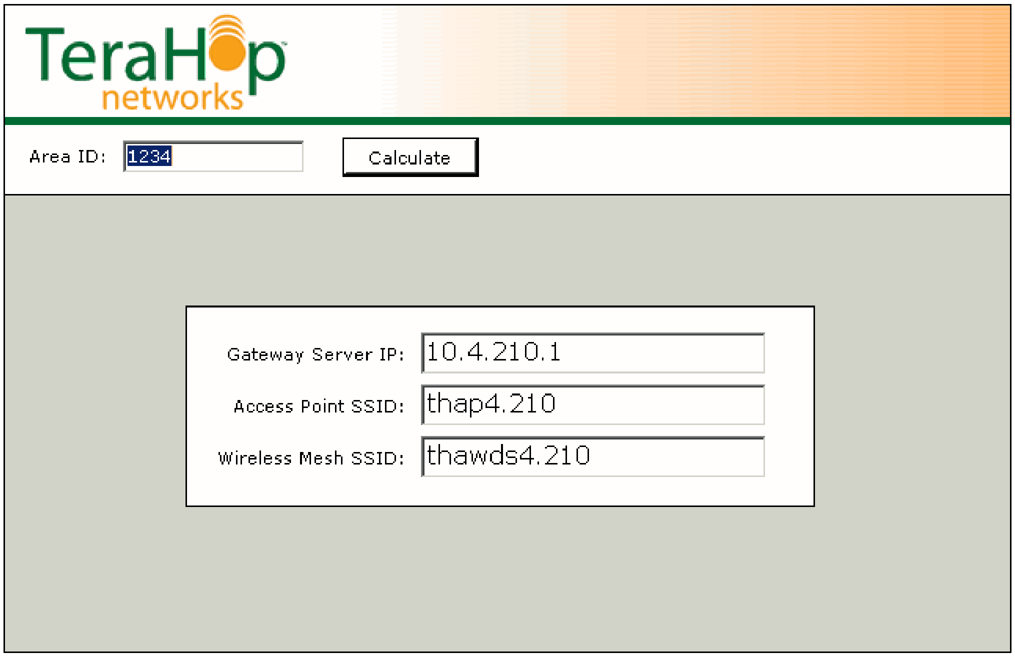


Enter the Area ID and click the Calculate button to find the Gateway Server's IP Address, the Access Point's SSID, and the Wireless Mesh's SSID.

2. In the **Area ID** text box, enter the Area ID for the system.
   The area ID can be found by looking on the label of the Gateway Router.

3. Click the **Calculate** button.
   The screen appears with the resulting addresses populated:
   Gateway Server IP
   Access Point SSID
   Wireless Mesh SSID

These values now should be used in the other portions of the MGS configuration.



Area ID: 1234

Gateway Server IP: 10.4.210.1

Access Point SSID: thap4.210

Wireless Mesh SSID: thawds4.210

Should you need to install the TeraHop Calculator, see Installing the TeraHop Calculator for MGS.

Should you need to manually determine the Wireless SSID, see Description of Mobile Gateway System (MGS) Wireless SSID Naming.

6.7 Description of Mobile Gateway System (MGS) Wireless SSID Naming

6.7.1 Wireless SSID Methodology

In order to connect the wireless components of the Mobile Gateway System (MGS), each must be configured with a matching SSID. On the Gateway Router, the access point and the wireless mesh SSIDs must be configured. Once completed, the PDA Client and administrative workstation running ADMS must also be configured. It is recommended that the access point and wireless mesh SSIDs follow the naming conventions provided by this document.

Each MGS uses two SSID. Each of those SSIDs must be unique, both inside the MGS and between MGSs. In order to achieve this, it is recommended that the MGS Access Point and Wireless Mesh are set using the Area ID as the base for the SSIDs.

The Access Point SSID should be set to thapA1.A2, where A1 and A2 are the second and third octet of the IP address assigned to the Gateway Router.

The Wireless Mesh SSID should be set to thawdsA1.A2, where A1 and A2 are the second and third octet of the IP address assigned to the Gateway Router.

To Calculate A1 and A2 please refer to Description of Mobile Gateway System IP Address Methodology.

If, for example, the Area ID (located on the label on the Gateway Server) is 1234, the resulting IP address would be 10.4.210.1. The Access Point's SSID should be thap4.210 and the Wireless Mesh's SSID should be thawds4.210.

Calculating A1 and A2 Scheme

	Hex	Dec
My Area ID		
A1		
A2		

The resulting IP Address is:

The Access Point SSID is:

The Wireless Mesh SSID is:

6.7.2 Configuring Mobile Gateway System SSIDs

The Mobile Gateway System (MGS) SSIDs are configured during application installation. Should the need arise to reset or change these settings, contact TeraHop Customer Service via e-mail or call 770-663-3455.

7.0 Using the IMS Software

7.1 The IMS Administration Station (ADMS)

The Administration Station (also called ADMS) provides an administrative tool for IMS system administrators to use in managing their IMS Mobile Gateway System, also called the MGS. This will also be used by Incident Command staff and NIMS-compliance personnel for configuring, querying, and updating the IMS. Channel Partners will use it for configuring, querying, and updating the system.

With ADMS, you can:

- Manage customer applications such as the IMS application
- Access network data
- Maintain and update network components
- Launch network component configuration applications such as the RSN Configuration Tool (RCT)
- Obtain system data logs

The ADMS is a laptop computer located at each customer facility home base (such as at a fire house). Some of the ADMS core functionality occurs automatically. For example, when a vehicle that houses an active Mobile Gateway System (MGS)arrives at the customer facility, the TDX application installed on the ADMS laptop computer automatically establishes a communication link with the MGS. Sensing any new data, the TDX automatically uploads the incident logs (and other MGS information) from the Mobile Gateway System. Other features of the ADMS are under user control and accessible either through the TeraHop Console or as standalone applications on the ADMS laptop computer.

7.2 The TeraHop Console

The TeraHop Console (THC) is a software framework from which you can access several TeraHop software applications and tools used in the setup and operation of the Incident Management System (IMS) *with* Automated Accountability. The THC is installed on the Administration Station (ADMS) laptop computer only.

From the TeraHop Console, you can start and run the following tools:

- RSN Configuration Viewer (RCV) to view configuration parameters from an attached RSN and display the data in a report.
- TeraHop Data Transfer (TDX) Tool, which is used to extract end-customer IMS incident logs;
- RSN Configuration Tool (RCT), which is used to set up end-customer configurations (including behavior settings that will govern an RSN's operation), and download a configuration to an RSN directly connected via a serial port.
- Gateway Configuration Tool (GCT), which is used to configure the settings (such as IP addresses) of the end-customer's Gateway Router (GR), Gateway Server (GS), and Mobile Messaging Router (MMR).

The THC add-ins are selected for installation when the TCH is installed. If you need to re-install it, please contact TeraHop Networks Customer Service.

The THC is pre-loaded on the ADMS laptop computer. If you need to reinstall it, please contact TeraHop Networks Customer Service.

The IMS PDA Application Configuration Tool (ACT), which is used to configure the application for the end customer, is a separate application residing on the ADMS laptop computer. The ACT is pre-loaded on the ADMS laptop computer. If you need to reinstall it, please contact TeraHop Networks Customer Service.

7.3 Working with the TeraHop Console and Its Applications

The TeraHop Console (THC) is used to launch tools and software applications that enable the user to set up and monitor the Incident Management System (IMS) *with* Automated Accountability.

The IMS system administrator has the following THC privileges:

- All non-administrators privileges
- Add non-administrator THC users and assign roles
- Change their own and THC user passwords
- Change the THC settings
- Add IMS add-ins
- Back up and restore the IMS database

Non-administrator users have the following THC privileges:

- Change their THC password
- Generate Incident Log reports using the THC add-in called TeraHop Data Transfer (TDX)
- Configure RSNs using the THC add-in called the RSN Configuration Tool (RCT)
- Configure the IMS application using the THC add-in called the Application Configuration Tool (ACT)
- View data using the RSN Configuration Viewer (RCV)

Administrator tasks are discussed in this section. Non-administrator tasks are discussed in subsequent sectionstopics.

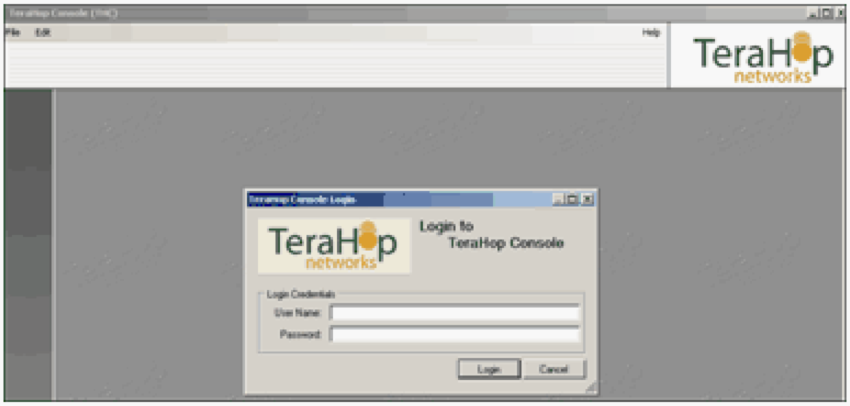
RSN Configuration Overview

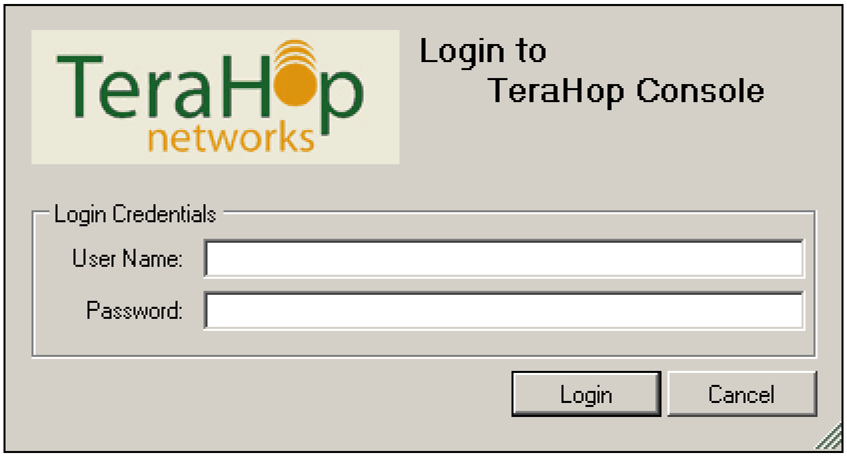
Creating IMS Application Configurations

7.4 How to Log Into the TeraHop Console

To log in to the TeraHop Console, do the following:

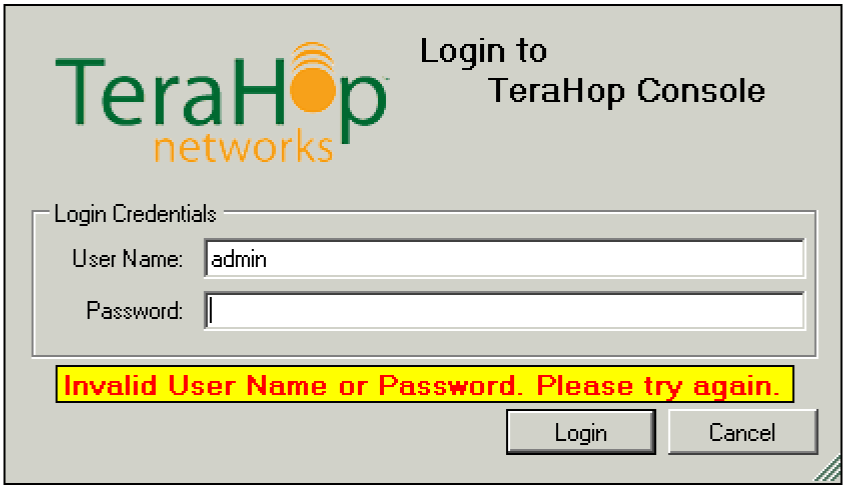
1. Double-click the THC icon.
   The **TeraHop Console** (THC) screen appears displaying the **TeraHop Console Login** window.





2. In the **User Name:** field, enter your user name.

3. In the **Password:** field, enter your password.
   Note: If you enter an invalid user name or password, the following message appears as illustrated below: *Invalid User name or Password Please try again*. Re-enter the password.

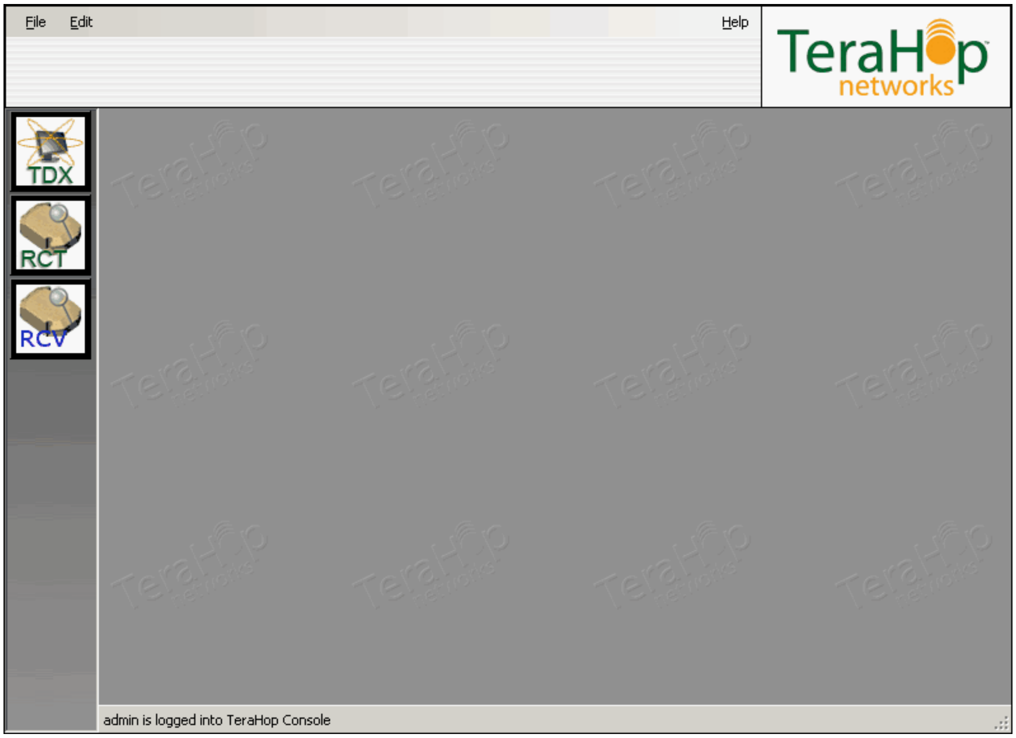


User Name: admin

Password:

Invalid User Name or Password. Please try again.

4. Click **Login**.
   The **THC** screen appears. On the left navigation pane are the add-ins that were selected during installation of the application.
   Note: Additional add-ins (such as the RSN Configuration Viewer (RCV) that you install will appear after you assign the roles (user privileges) for that add-in. In the example below, the Administration Station (ADMS) and RSN Configuration Tool (RCT) add-ins appear. See How to Add Non-administrator THC Users.



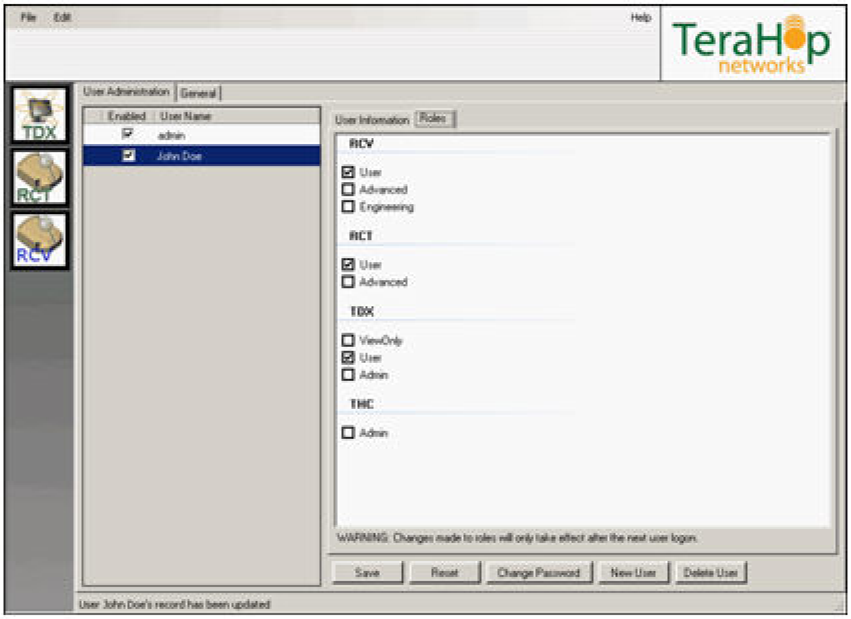
admin is logged into TeraHop Console

5.

7.5 How to Add Non-administrator THC Users

To add non-administrator THC users, do the following:

1. From the **File** menu, select **Settings**.
   The **User Administration** tab appears.



Enabled	User Name
☑	admin
☑	John Doe

RCV

☑ User
□ Advanced
□ Engineering

RCT

☑ User
□ Advanced

TDX

□ ViewOnly
☑ User
□ Admin

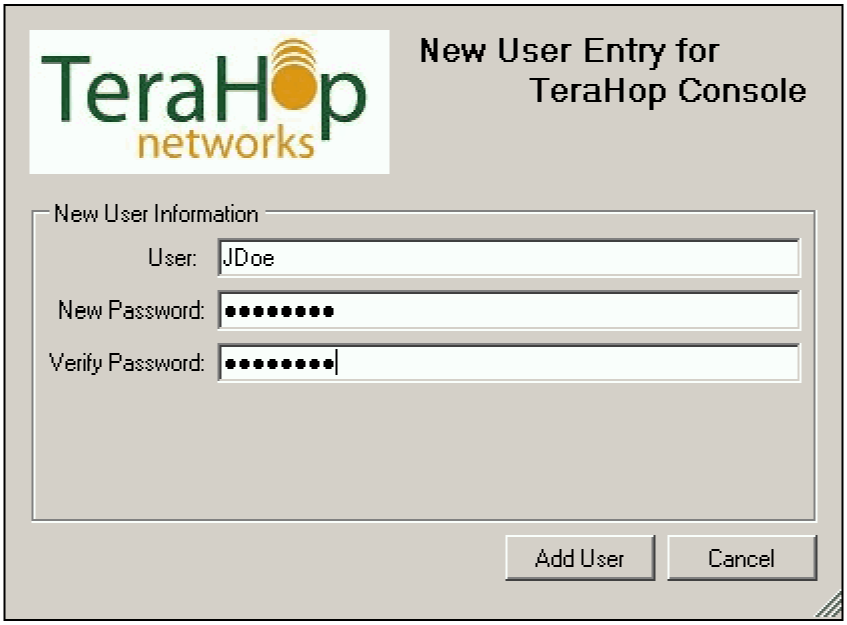
THC

□ Admin

WARNING: Changes made to roles will only take effect after the next user logon.

User John Doe's record has been updated

2. On the bottom of the screen, click **New User**.
   The **New User Entry for TeraHop Console** dialog box opens.



New User Entry for TeraHop Console

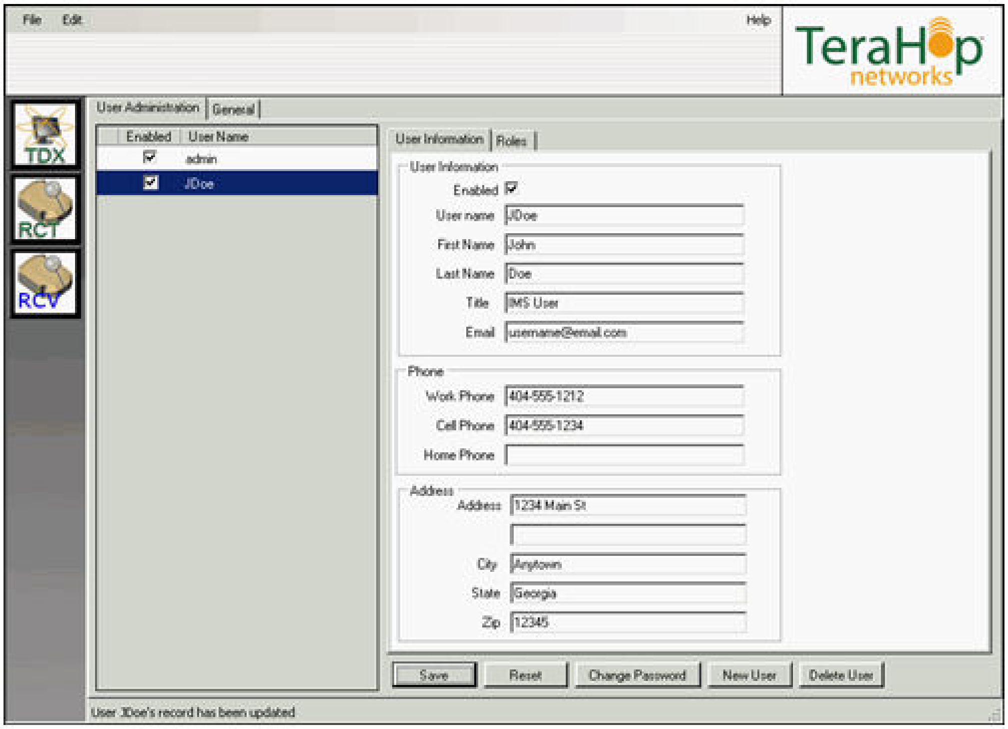
New User Information

User: JDoe

New Password: ●●●●●●●●●

Verify Password: ●●●●●●●●●

3. In the **User:** field, enter a user name for this new user.
   The user name is case insensitive and can be from 1 to 50 characters of any kind (except ' or ").
4. In the **New Password:** field, enter a password.
   The password is case sensitive and must be from 6 to 40 characters.
5. In the **Verify Password:** field, repeat the password.
6. Click **Add User**.
   The **User Information** tab appears with blank fields.
7. Under **User Information**, click the **Enabled** check box to activate this user.
8. Complete the fields on the **User Information** tab.



Enabled	User Name
☑	admin
☑	JDoe

User Information

Enabled ☑

User name: JDoe

First Name: John

Last Name: Doe

Title: IMS User

Email: username@email.com

Phone

Work Phone: 404-555-1212

Cell Phone: 404-555-1234

Home Phone:

Address

Address: 1234 Main St

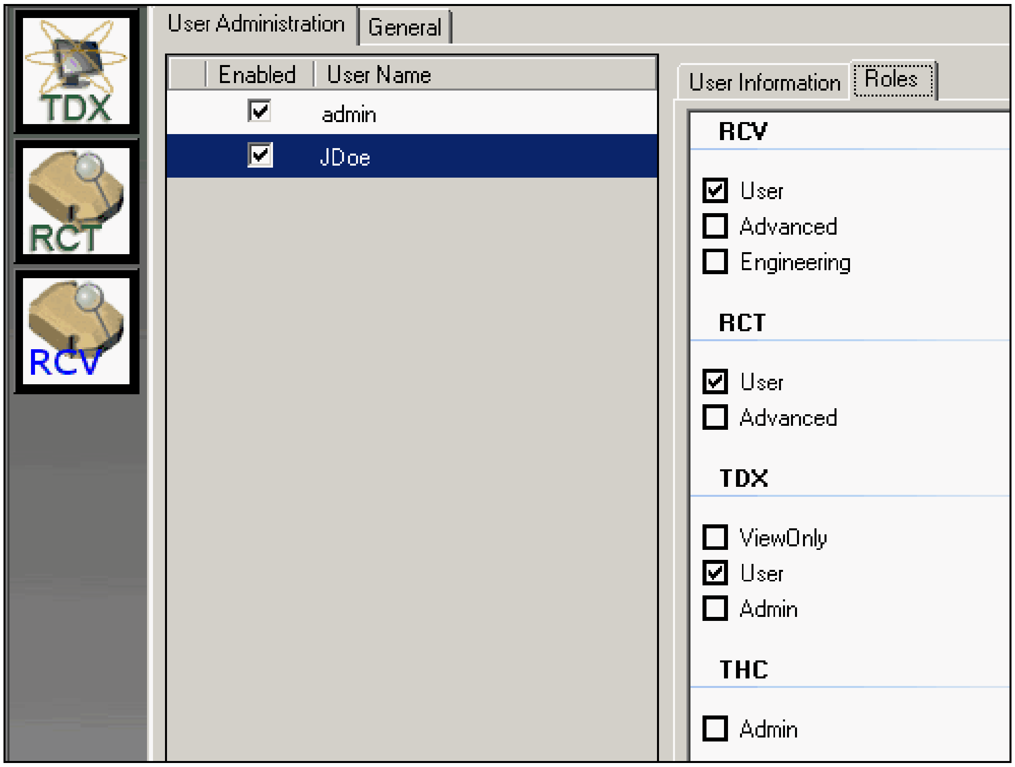
City: Anytown

State: Georgia

Zip: 12345

User JDoe's record has been updated

9. Click the **Roles** tab.



Enabled	User Name
☑	admin
☑	JDoe

RCV

☑ User
□ Advanced
□ Engineering

RCT

☑ User
□ Advanced

TDX

□ ViewOnly
☑ User
□ Admin

THC

□ Admin

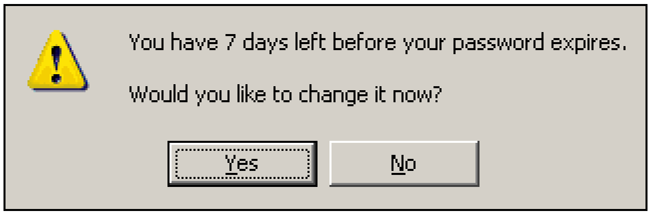
10. For each add-in, select the level of user privilege (the role) by clicking the checkbox. For example: **ViewOnly**, **User**, or **Admin**.

11. In the left pane **User Administration** tab, under **Enabled**, select the checkbox next to JDoe.
    You must select **Enabled** so that this user is an active user. If you decide later that you want to disable this user, you can disable the user by clearing (deselecting) the **Enabled** check box without having to remove the user. This also allows you to re-enable the user without having to reenter all of the user information.

12. Click **Save**.
    The new user is added to the THC and can now log in and perform the tasks associated with the level of privileges you gave them. The following message appears in the lower left portion of the screen: *User JDoe's (username) record has been updated.*
    Note: If you change a user's roles (including an Admin's), the changes will not take affect until the user logs out of the THC and logs back in.

7.6 How to Change Passwords in the TeraHop Console

Passwords expire after 30 days. Every time a user logs in to the THC, the login dialog box displays the number of days until the password expires.



You have 7 days left before your password expires.

Would you like to change it now?

The THC administrator can change anyone's password. A THC user can change their own password.

For the THC administrator to change a THC user's password, do the following:

1. From the **File** menu, select **Settings**.
2. In the **User Administration** pane, select the name of the user whose password is to be changed.
   The user's data appears in the User Information tab on the right.
3. On the bottom of the screen, click **Change Password**.
   The **Change Password to TeraHop Console** dialog box opens displaying the name of the user.
4. In the **New Password** field, enter the new password, and confirm it by entering it again in the **Verify Password** field.
   Note: Passwords are case sensitive.

For a user to change their own password, the user does the following:

1. Log in.
2. From the **File** menu, select **Settings**.
3. From the **Edit** menu, select **Change Password**.
   The **Change Password to TeraHop Console** dialog box opens displaying the user's name.
4. In the **New Password** field, enter the new password, and confirm it by entering it again in the **Verify Password** field.
   Note: Passwords are case sensitive.

7.7 How to Disable or Delete a THC User

Depending on the circumstances, it may be advantageous to disable a user instead of deleting them. This may be used if a person is on a leave of absence.

To deactivate a THC user, do the following:

1. From the **File** menu, select **Settings**.
2. On the **User Administration** tab, under **Enabled**, select the checkbox next to the name of the person to be disabled.
   The fields on the **User Information** tab populate with the user's data.
3. On the **User Information** tab, clear (deselect) the **Enabled** checkbox.
4. Click **Save**.

To delete a THC user, do the following:

From the **File** menu, select **Settings**.

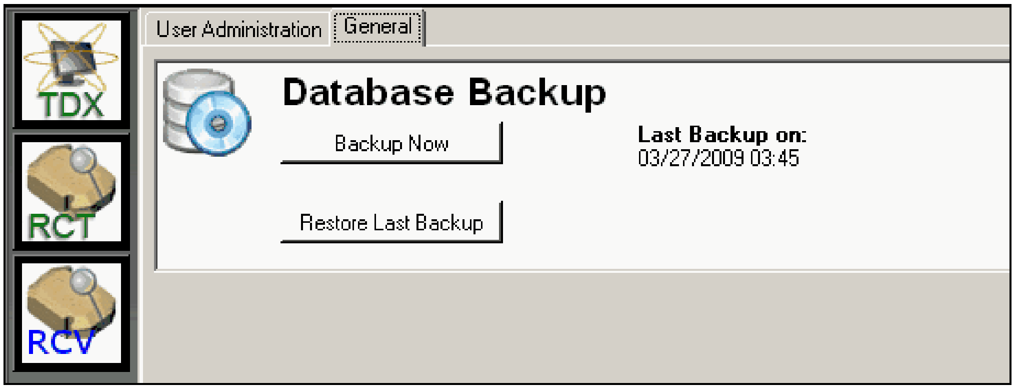
1. On the **User Administration** tab, under **Enabled**, select the checkbox next to the name of the person to be deleted.
   The fields on the **User Information** tab populate with the person's data.
2. To delete the person, click **Delete User**.
   The **Delete User?** popup appears displaying the following message: *Are you sure you want to delete user JDoe (username)?*
3. To confirm the deletion, click **OK**.
   The person's data will be cleared from the screen and the THC.
4. To cancel the deletion, click **No**.

7.8 How to Back Up the THC Database

TeraHop Networks recommends that you back up the SQL database on a regular basis according to your standard system maintenance and back-up policies. The backup described below enables you to retrieve a previous version of the SQL database. The database is backed up to the same hard drive on the laptop computer on which the THC is installed. The database is backed up to C:\Program Files\Microsoft SQL Server\MSSQL.1\Backup\THCConsole.bak.

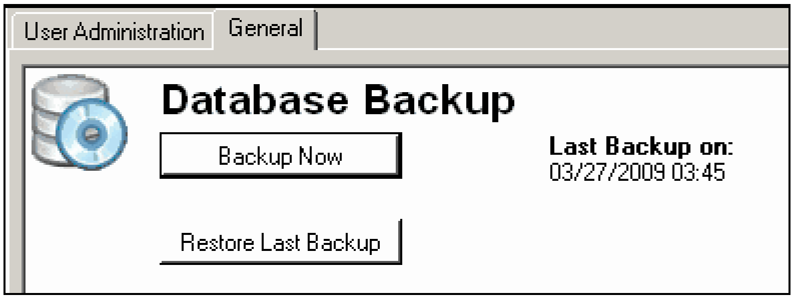
To back up the THC database, do the following:

1. From the **File** menu, select **Settings**.
2. Click the **General** tab.
   The **Database Backup** screen appears displaying the date and time of the last database backup.



Last Backup on:
03/27/2009 03:45

3. To back up the database, click **Backup Now**.
   The *Last Backup on:* message changes to reflect the date and time of the backup.



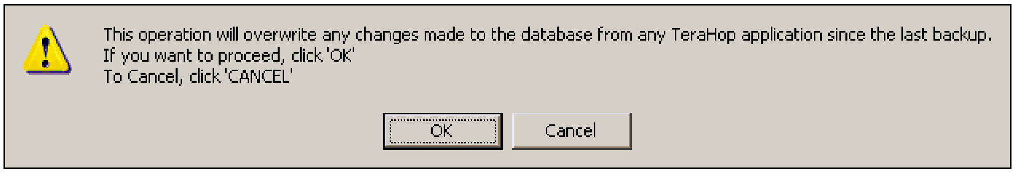
Last Backup on:
03/27/2009 03:45

7.9 How to Restore the THC Database

You may restore the previous version of the SQL database.

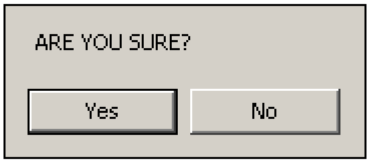
To restore a backed up THC database, do the following:

1. From the **File** menu, select **Settings**.
2. Click the **General** tab.
   The **Database Backup** screen appears displaying the date and time of the last database backup.
3. Click **Restore Last Backup**.
   The following confirmation message appears:



This operation will overwrite any changes made to the database from any TeraHop application since the last backup.
If you want to proceed, click 'OK'
To Cancel, click 'CANCEL'

4. To cancel the operation, click **Cancel**.
5. To restore the previous version of the SQL database, click **OK**.
   A second confirmation message appears.



ARE YOU SURE?

6. If you are absolutely sure you want to restore the SQL database, click **Yes**.
7. If you are not absolutely sure you want to restore the SQL database, click **No**.

7.10 Working with the RSN Configuration Viewer (RCV)

The RSN Configuration Viewer (RCV) is a TeraHop Console (THC) add-in application that reads configuration and parameter data from a specific RSN and displays the data in a report that may be printed or e-mailed.

The RCV works with the RCT Cradle.

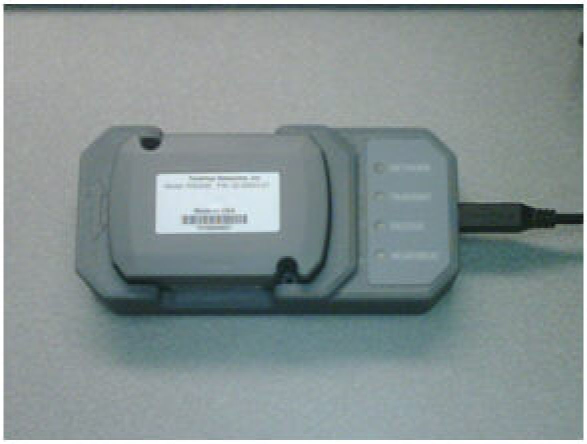


Figure 13: RSN in RCT Cradle

You can complete reading the configuration data for one RSN, and then move immediately on to reading the next RSN. After reading RSN data, you can save the data to a file and e-mail the file to another person.

Note: Viewing the RSN data with the RCV does NOT alter the configuration of the RSN being read.

Depending on your assigned user role, the RCV displays the following RSN data:

- Primary class
- First Responder indicator
- THC Customer ID and RSN Customer ID
- User data block(s)
- Each Behavioral Profile (total of three for User and Advanced roles; 16 for Engineering roles)
- The four potential sensor events (Check-in, Shock, Motion, and No-Motion) for User and Advanced roles
- The 16 potential sensor events for Engineering roles
- The six parameters for each sensor (Event Trigger, Sensor Configuration, Period, Maintain, Reporting Period, and Magnitude Limit).
- Unit ID (UID)

- Software version
- Hardware version
- Configuration version
- Customer ID, Customer Name
- Sled Information

To use the RCV, you must be logged into the THC. You must have permission from your administrator to use the RCV. If you do not see the RCV icon on the THC after logging in, see your system administrator, who will assign you the proper role that will enable you to use the RCV.

See also:

How to View RSN Parameters with the RCV

Types of RSN Configuration Data You Can View

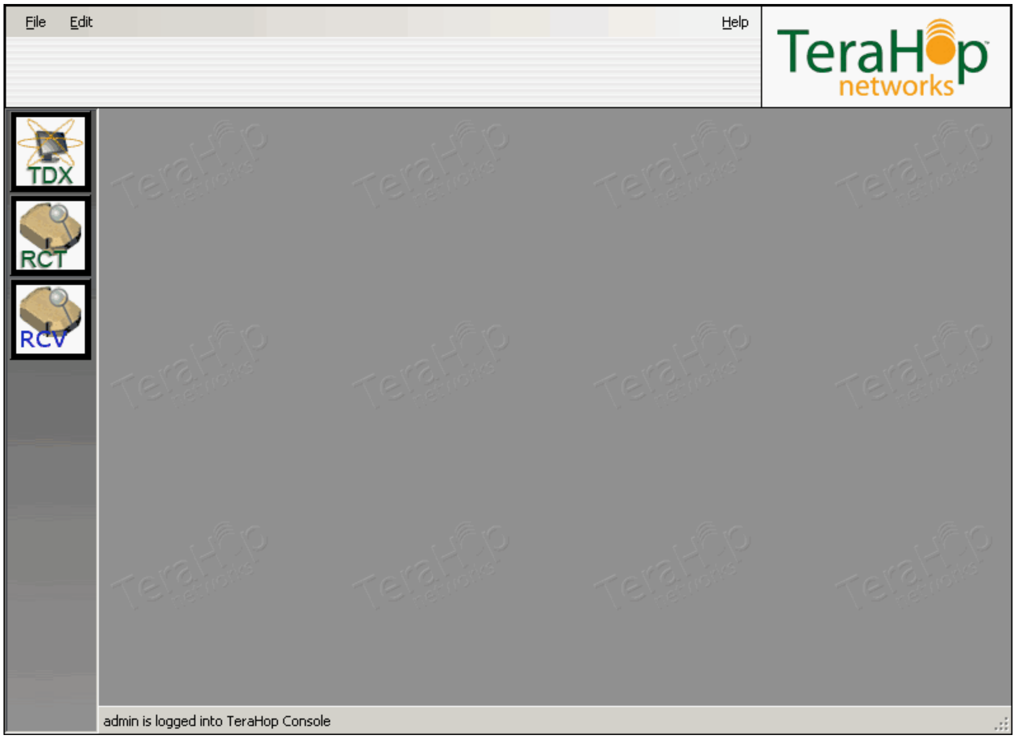
Sending RSN Configuration Data to TeraHop Networks Customer Service

7.11 How to View RSN Parameters with the RSN Configuration Viewer (RCV)

Note: If the RCT cradle and the USB are connected to the ADMS laptop computer before launching the RCV, the COM port is automatically pre-selected.

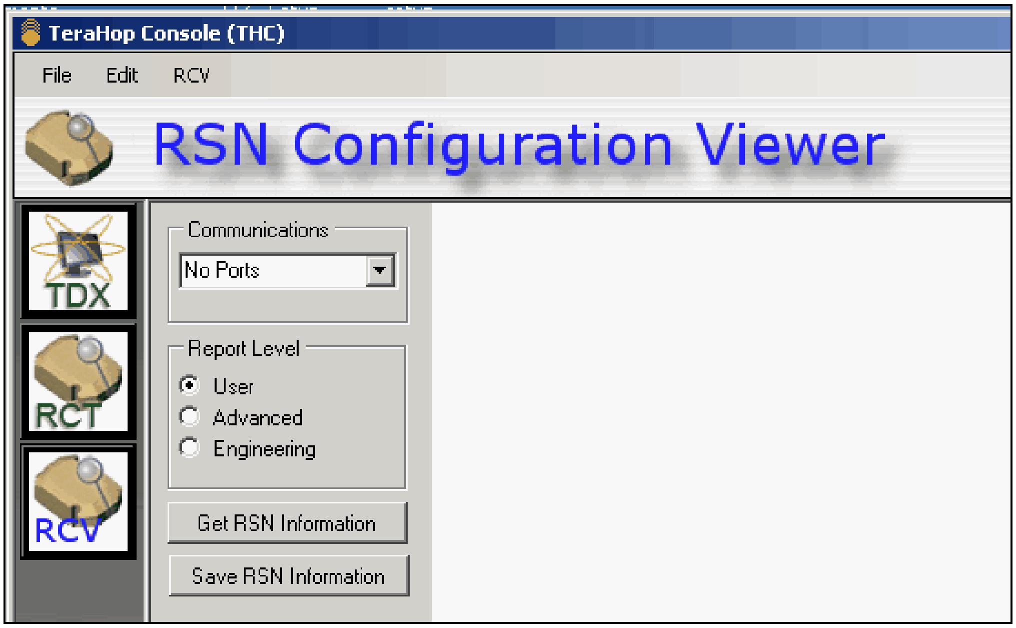
To view an RSN configuration, do the following:

1. Log into the THC.



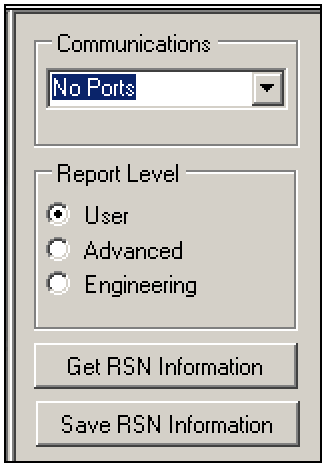
admin is logged into TeraHop Console

2. Click the **RCV** icon.
   The **RSN Configuration Viewer** screen appears.



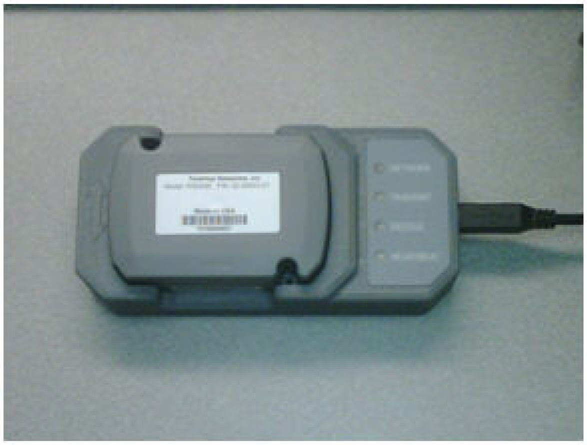
3. Connect the RCT Cradle to the computer on which the THC resides using the USB cable provided with the RCT Cradle.
   Note: You will not see any lights on the RCT Cradle until an RSN is placed in the cradle.

4. On the **RSN Configuration Viewer** screen, under **Communications** click the drop-down-arrow and select the communications port to which the RCT Cradle is connected.



5. Remove the plug from the back of the RSN and set the plug and the screws aside.

6. Place the RSN whose data you want to read in the RCT Cradle as shown below. Ensure that the connector end of the RSN makes contact with the connector in the cradle.



The Heartbeat and Receive LEDs on the RCT Cradle should blink.

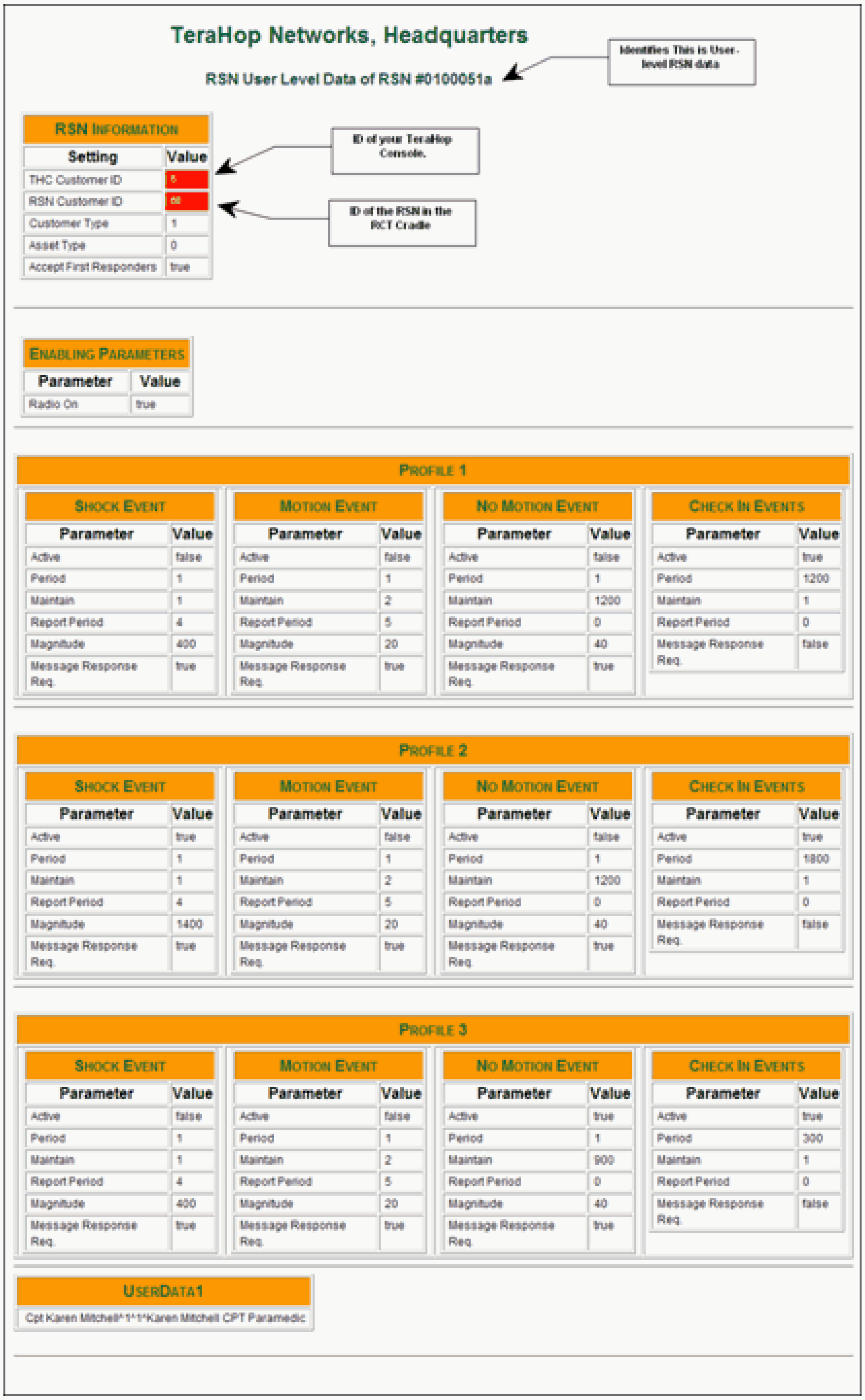
7.12 Types of RSN Data You Can View

7.12.1 Displaying User-Level RSN Data

Depending on the role assigned to you for the RCV, you can view either user-level, advanced-level, or engineering-level RSN data.

1. To display user-level RSN data, on the **RSN Configuration Viewer** screen, under **Report Level**, select the **User** radio button.
2. Click **Get RSN Information**.

The screen displays user-level information about the data in the RSN as illustrated below.



TeraHop Networks, Headquarters

RSN User Level Data of RSN #0100051a

Identifies This is User-level RSN data

ID of your TeraHop Console.

ID of the RSN in the RCT Cradle

RSN Information

Setting	Value
THC Customer ID	5
RSN Customer ID	68
Customer Type	1
Asset Type	0
Accept First Responders	true

Enabling Parameters

Parameter	Value
Radio On	true

Profile 1

Shock Event

Parameter	Value
Active	false
Period	1
Maintain	1
Report Period	4
Magnitude	400
Message Response Req.	true

Motion Event

Parameter	Value
Active	false
Period	1
Maintain	2
Report Period	5
Magnitude	20
Message Response Req.	true

No Motion Event

Parameter	Value
Active	false
Period	1
Maintain	1200
Report Period	0
Magnitude	40
Message Response Req.	true

Check In Events

Parameter	Value
Active	true
Period	1200
Maintain	1
Report Period	0
Message Response Req.	false

Profile 2

Shock Event

Parameter	Value
Active	true
Period	1
Maintain	1
Report Period	4
Magnitude	1400
Message Response Req.	true

Motion Event

Parameter	Value
Active	false
Period	1
Maintain	2
Report Period	5
Magnitude	20
Message Response Req.	true

No Motion Event

Parameter	Value
Active	false
Period	1
Maintain	1200
Report Period	0
Magnitude	40
Message Response Req.	true

Check In Events

Parameter	Value
Active	true
Period	1800
Maintain	1
Report Period	0
Message Response Req.	false

Profile 3

Shock Event

Parameter	Value
Active	false
Period	1
Maintain	1
Report Period	4
Magnitude	400
Message Response Req.	true

Motion Event

Parameter	Value
Active	false
Period	1
Maintain	2
Report Period	5
Magnitude	20
Message Response Req.	true

No Motion Event

Parameter	Value
Active	true
Period	1
Maintain	900
Report Period	0
Magnitude	40
Message Response Req.	true

Check In Events

Parameter	Value
Active	true
Period	300
Maintain	1
Report Period	0
Message Response Req.	false

UserData1

Cpt Karen Mitchell^1^1^Karen Mitchell CPT Paramedic

The screen displays information as follows:

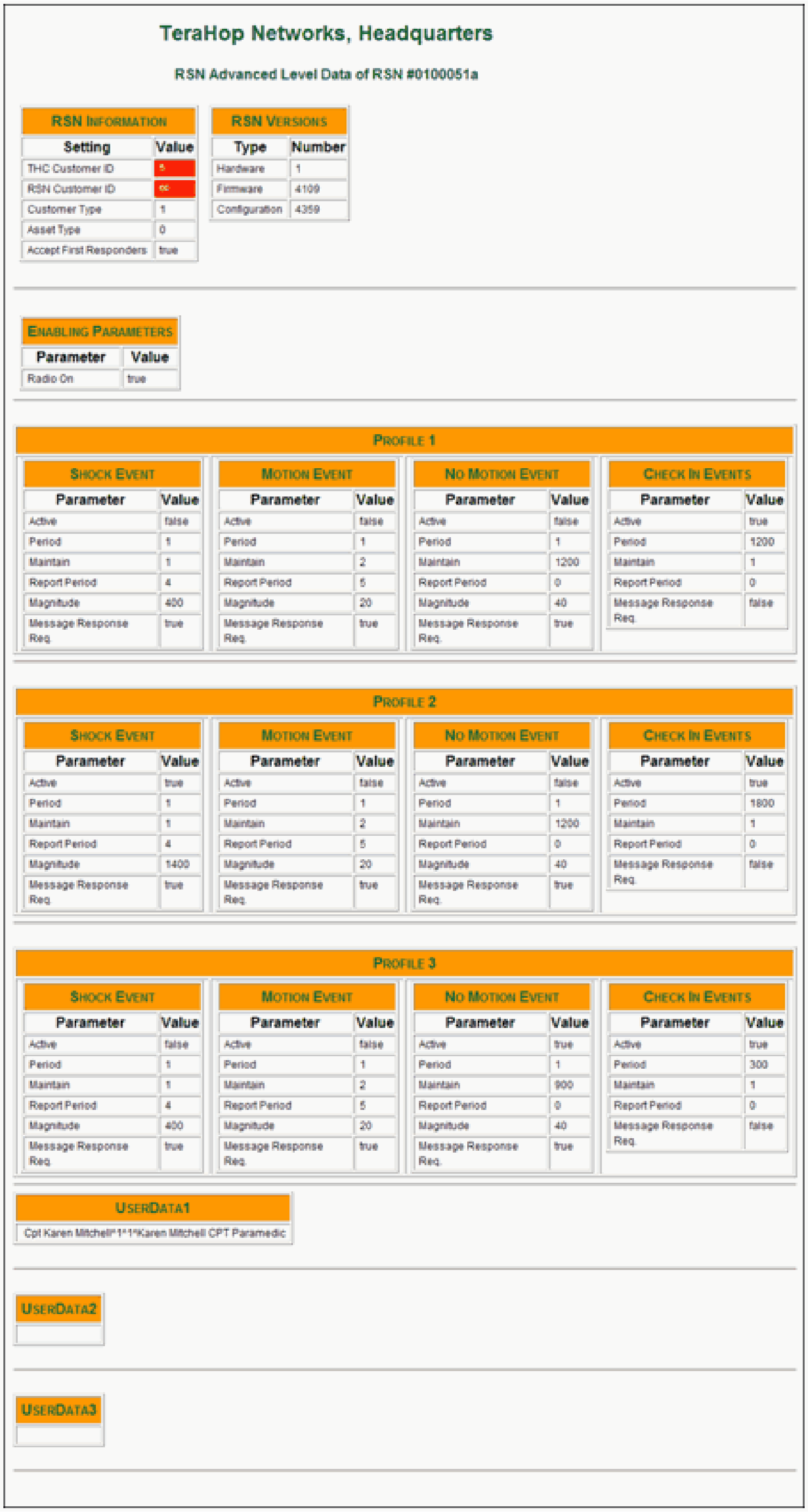
RSN Information box: Basic RSN information appears. If the THC Customer ID and the RSN Customer ID are different, these boxes appear red. This means that the RSN was programmed with a Customer ID other than yours. If the RSN field is zero, the RSN has not been programmed. If the RSN has not been programmed, all Profile fields are zeros, the factory default.

Profile 1, Profile 2, and Profile 3 boxes: These are the behavior profiles for the RSN. A behavior profile defines the behavior of the RSN as it encounters situations while in use in the field.

UserData1 box: displays data specific to the owner of that RSN. This may be personal data, such as a name or data about the item to which the RSN is attached, such as a vehicle or piece of equipment.

7.12.2 Displaying Advanced-Level RSN Data

1. To display advanced-level RSN data, on the **RSN Configuration Viewer** screen, under **Report Level**, select the **Advanced** radio button.
2. Click **Get RSN Information**.
   The screen displays advanced-level information about the data in the RSN as illustrated on the next page.



TeraHop Networks, Headquarters

RSN Advanced Level Data of RSN #0100051a

RSN Information

Setting	Value
THC Customer ID	5
RSN Customer ID	cc
Customer Type	1
Asset Type	0
Accept First Responders	true

RSN Versions

Type	Number
Hardware	1
Firmware	4109
Configuration	4359

Enabling Parameters

Parameter	Value
Radio On	true

Profile 1

Shock Event

Parameter	Value
Active	false
Period	1
Maintain	1
Report Period	4
Magnitude	400
Message Response Req.	true

Motion Event

Parameter	Value
Active	false
Period	1
Maintain	2
Report Period	5
Magnitude	20
Message Response Req.	true

No Motion Event

Parameter	Value
Active	false
Period	1
Maintain	1200
Report Period	0
Magnitude	40
Message Response Req.	true

Check In Events

Parameter	Value
Active	true
Period	1200
Maintain	1
Report Period	0
Message Response Req.	false

Profile 2

Shock Event

Parameter	Value
Active	true
Period	1
Maintain	1
Report Period	4
Magnitude	1400
Message Response Req.	true

Motion Event

Parameter	Value
Active	false
Period	1
Maintain	2
Report Period	5
Magnitude	20
Message Response Req.	true

No Motion Event

Parameter	Value
Active	false
Period	1
Maintain	1200
Report Period	0
Magnitude	40
Message Response Req.	true

Check In Events

Parameter	Value
Active	true
Period	1800
Maintain	1
Report Period	0
Message Response Req.	false

Profile 3

Shock Event

Parameter	Value
Active	false
Period	1
Maintain	1
Report Period	4
Magnitude	400
Message Response Req.	true

Motion Event

Parameter	Value
Active	false
Period	1
Maintain	2
Report Period	5
Magnitude	20
Message Response Req.	true

No Motion Event

Parameter	Value
Active	true
Period	1
Maintain	900
Report Period	0
Magnitude	40
Message Response Req.	true

Check In Events

Parameter	Value
Active	true
Period	300
Maintain	1
Report Period	0
Message Response Req.	false

UserData1

Cpt Karen Mitchell*1*1*Karen Mitchell CPT Paramedic

UserData2

UserData3

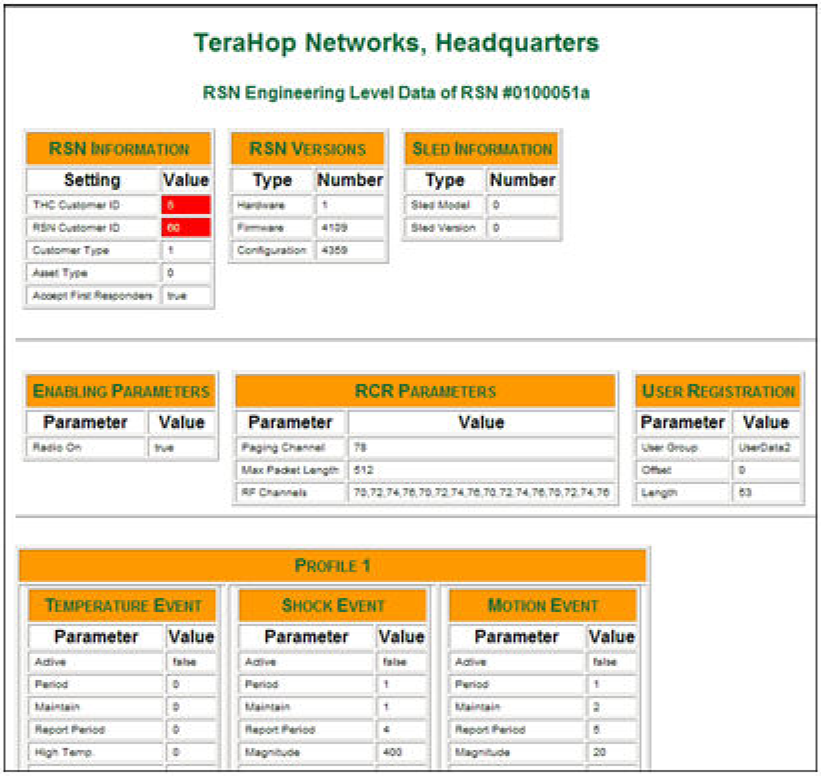
In addition to the data on the user-level screen, the advanced-level screen includes the **RSN Version** box, which includes the version number of the RSN hardware, firmware, and configuration.

The UserData2 and UserData3 boxes are not used at this time.

7.12.3 Displaying Engineering-Level RSN Data

To display engineering-level RSN data, do the following:

1. On the RSN Configuration Viewer screen, under Report Level, select the Engineering radio button.
2. Click **Get RSN Information**.
   The screen displays engineering-level information about the data in the RSN as illustrated below.



TeraHop Networks, Headquarters

RSN Engineering Level Data of RSN #0100051a

RSN INFORMATION

Setting	Value
THC Customer ID	0
RSN Customer ID	00
Customer Type	1
Asset Type	0
Accept First Responders	true

RSN VERSIONS

Type	Number
Hardware	1
Firmware	4109
Configuration	4359

SLED INFORMATION

Type	Number
Sled Model	0
Sled Version	0

ENABLING PARAMETERS

Parameter	Value
Radio On	true

RCR PARAMETERS

Parameter	Value
Paging Channel	79
Max Packet Length	512
RF Channels	70,72,74,76,70,72,74,76,70,72,74,76,70,72,74,76

USER REGISTRATION

Parameter	Value
User Group	UserData2
Offset	0
Length	53

PROFILE 1

TEMPERATURE EVENT

Parameter	Value
Active	false
Period	0
Maintain	0
Report Period	0
High Temp.	0

SHOCK EVENT

Parameter	Value
Active	false
Period	1
Maintain	1
Report Period	4
Magnitude	400

MOTION EVENT

Parameter	Value
Active	false
Period	1
Maintain	2
Report Period	5
Magnitude	20

In addition to the data displayed on the Advanced-level screen, the Engineering-level screen displays the following data:

Sled Information: displays information about the RCT Cradle in which the RSN resides.

RCR Parameters: displays the radio parameter used to communicate from the Gateway Router (GR) to the RSN.

User Registration: specifies which user data area and how much data is broadcast on registration, used in construct with user data areas.

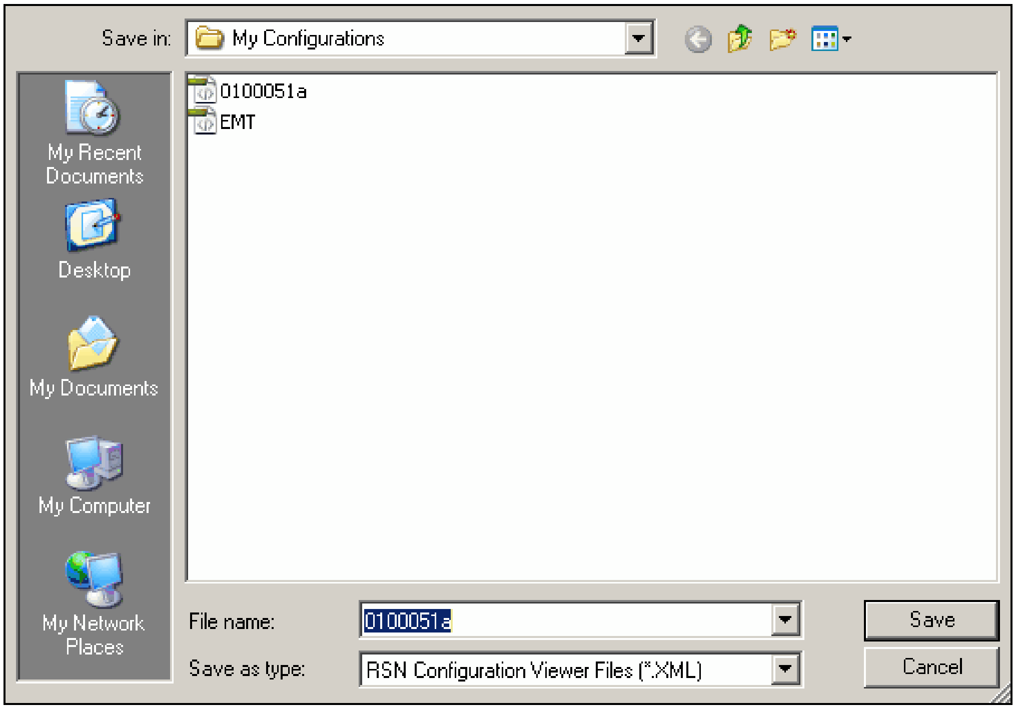
All 16 possible profiles: displays each of the 16 profiles that are possible for the RSN.

7.13 Saving RSN Configuration Data to a File

You can save the RSN configuration data to an XML file and then view it in an XML viewer or in the RCV.

To save the RSN configuration data, do the following:

1. Ensure that the RSN is in the RCT Cradle and that you have clicked **Get RSN Information**.
2. Click **Save RSN Information**.
   The **Save As** dialog box opens displaying the RSN Unit ID as the default file name. RCV is set up to save this file to a folder on your computer called **My Configurations.**



Save in: My Configurations

0100051a

EMT

File name: 0100051a

Save as type: RSN Configuration Viewer Files (*.XML)

3. To save this file to a different folder, click the **Save in:** field drop-down arrow, and browse to the folder to which you want to save this file.
4. Click **Save**.

Viewing a Saved RSN Configuration Data File

You can view a saved file with an XML viewer or in the RCV.

To view a saved RCV file, do the following:

1. To view the file, browse to the location on the computer to which you saved the file.
2. Right-click the file and select **Open with**.

3. Open the file with your favorite XML viewer.
   or
4. To open the file in RCV, in the THC click the **File** menu and select **Open**.
   The **My Configurations Open** dialog box opens.
5. Select the Unit ID of the file you want to view, and click **Open**.
   The file opens in the RCV.

7.14 TeraHop Data Transfer (TDX)

During an incident, the IMS system collects and stores information regarding the transmission and disposition of messages between the various components. Two types of data are stored. The first is the Incident Log that provides a time sequenced, easy to read chronological log of the event that have taken place. The second type of data is a time sequenced log of the interworkings of the network.

At the end of an incident, the MMR-equipped vehicle returns to the station or garage and the Incident Commander and other personnel return to their office or go about their other duties. The data stored in the vehicle’s MMR is then automatically transferred from the vehicle to the ADMS laptop computer (requires the THC to be active). These data transfers include Incident Logs, System Event Logs, MDRs, and Queue Journals (if enabled).

To extract, view and save the Incident Log, the TeraHop Data Transfer (TDX) add-in on the THC is used.

The IMS application creates an Incident Log during an incident within the IMS application. The Incident Log records and timestamps each event from the RSNs and actions from the Incident Commander (IC) in an easy-to-read format.

The Incident Log captures:

- Start of the Incident
- Incident Information: name, incident type, description, location
- Arrival of all assets
- All assignments and reassignments of the assets
- Distress alerts
- Departure of assets (the loss of contact)
- Notes created by the IC
- RSN low and critical battery alerts
- Assets that are added manually and managed by the IC
- Termination of the incident

The TDX has an easy-to-use user interface where the user inputs the date/time ranges of interest. The tool returns the incident names that occurred within that time range. The user can then select the appropriate incident number and/or the time range of interest and the tool creates an Incident Report in a .pdf format that can be viewed and printed by the user.

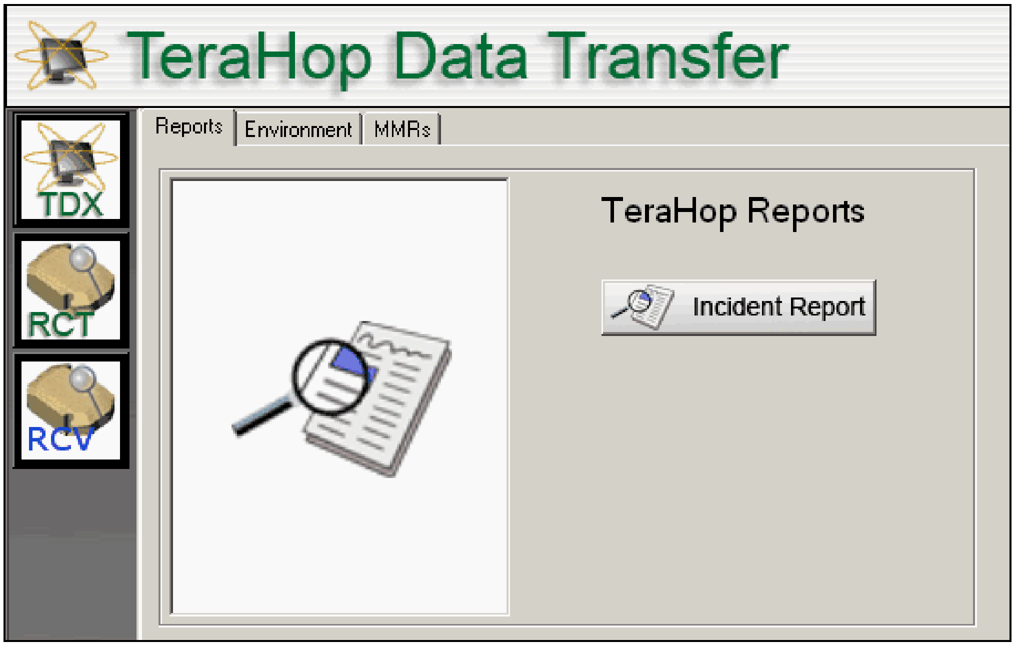
The printed report can later be appended to the standard National Incident Management System (NIMS) Report.

For instructions on generating the Incident Report, go to How to Extract an Incident Log.

7.15 How to Extract an Incident Report

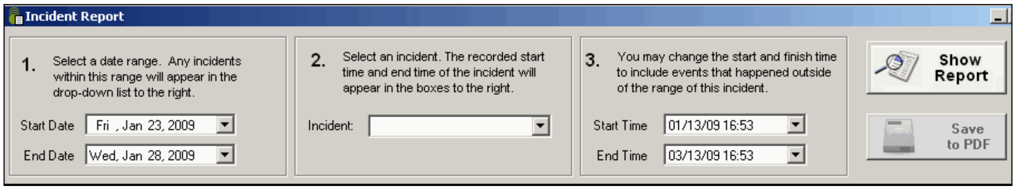
The incident report is available through the TeraHop Data Transfer (TDX) Tool application that resides on the TeraHop Console (THC).

1. To extract an incident report, do the following:
2. On the THC, click the **TDX** icon.
   The **TeraHop Data Transfer** screen appears.



3. On the **Reports** tab, click **Incident Report**.

   The laptop communicates wirelessly with the MMR at the database level to extract data.
   The **Incident Report** window opens in a new window. Across the top of the screen in a new window you will see three sections labeled 1, 2, and 3.



1. Select a date range. Any incidents within this range will appear in the drop-down list to the right.

Start Date: Fri , Jan 23, 2009
End Date: Wed, Jan 28, 2009

2. Select an incident. The recorded start time and end time of the incident will appear in the boxes to the right.

Incident:

3. You may change the start and finish time to include events that happened outside of the range of this incident.

Start Time: 01/13/09 16:53
End Time: 03/13/09 16:53

4. In section 1, click the drop-down arrows to select a data range for the incident you want to view.
   The incidents that occurred in the range you entered will appear in a drop-down list in section 2.

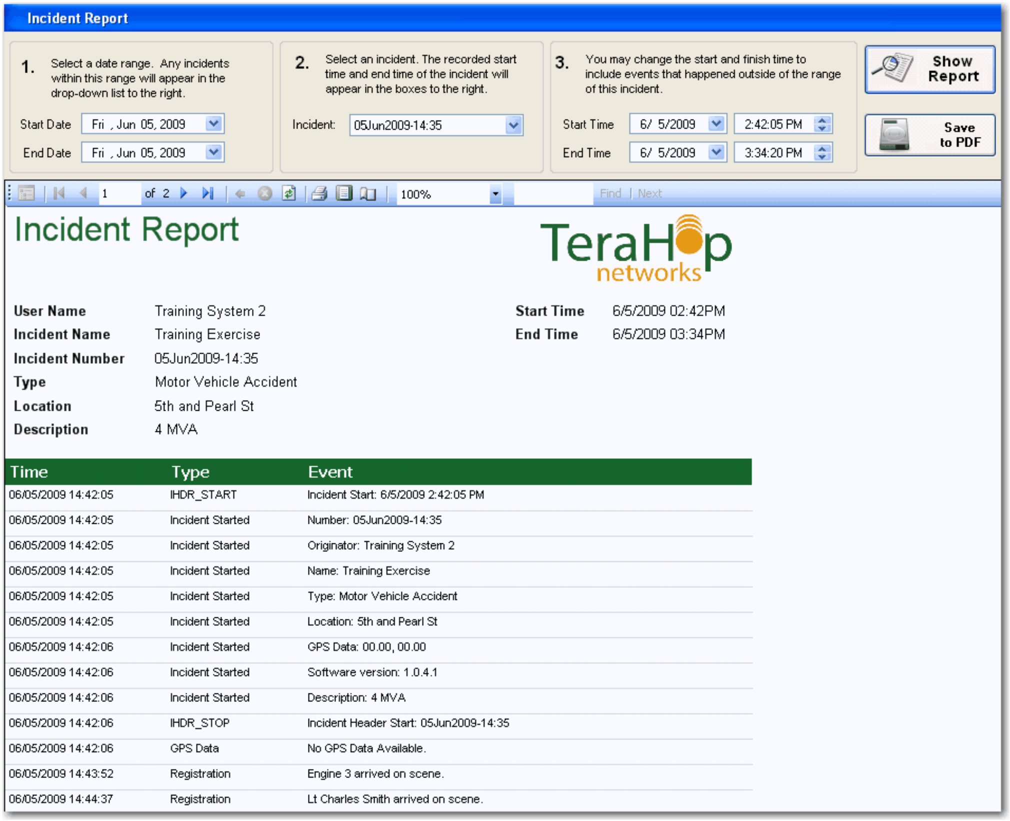
You may select an event from section 2 or you can select to view data between specific start and end incident times by using section 3.

5. To select a specific event, in section 2 click the drop-down arrow and select an incident.
   The start and end times for the event will appear on the right in section 3. You can click **Show Report** to show all the data for this event.

6. To include or exclude events which occurred before or after an incident event, in section 3, you can change the start and end time for the date you selected in section 2. For example, you may have an incident after the main incident called Cleanup. If you want to include the Cleanup incident in your report, you may select the end time to be after the Cleanup incident. This enables you to merge the data from two incidents into one report.

   The data for the incident you selected is pulled from the database.

7. Click **Show Report**.
   The data for the incident appears on the screen.



1. Select a date range. Any incidents within this range will appear in the drop-down list to the right.

Start Date Fri , Jun 05, 2009
End Date Fri , Jun 05, 2009

2. Select an incident. The recorded start time and end time of the incident will appear in the boxes to the right.

Incident: 05Jun2009-14:35

3. You may change the start and finish time to include events that happened outside of the range of this incident.

Start Time 6/ 5/2009 2:42:05 PM
End Time 6/ 5/2009 3:34:20 PM

Incident Report

User Name	Training System 2	**Start Time**	6/5/2009 02:42PM
Incident Name	Training Exercise	**End Time**	6/5/2009 03:34PM
Incident Number	05Jun2009-14:35		
Type	Motor Vehicle Accident		
Location	5th and Pearl St		
Description	4 MVA		

Time	Type	Event
06/05/2009 14:42:05	IHDR_START	Incident Start: 6/5/2009 2:42:05 PM
06/05/2009 14:42:05	Incident Started	Number: 05Jun2009-14:35
06/05/2009 14:42:05	Incident Started	Originator: Training System 2
06/05/2009 14:42:05	Incident Started	Name: Training Exercise
06/05/2009 14:42:05	Incident Started	Type: Motor Vehicle Accident
06/05/2009 14:42:05	Incident Started	Location: 5th and Pearl St
06/05/2009 14:42:06	Incident Started	GPS Data: 00.00, 00.00
06/05/2009 14:42:06	Incident Started	Software version: 1.0.4.1
06/05/2009 14:42:06	Incident Started	Description: 4 MVA
06/05/2009 14:42:06	IHDR_STOP	Incident Header Start: 05Jun2009-14:35
06/05/2009 14:42:06	GPS Data	No GPS Data Available.
06/05/2009 14:43:52	Registration	Engine 3 arrived on scene.
06/05/2009 14:44:37	Registration	Lt Charles Smith arrived on scene.

8. To save the report to a .pdf file, click **Save As** and browse to the location where you want to save this file.

9. Click **OK**.
   The file will be saved.

8.0 Configuring the System

8.1 Configuring the IMS Application (ACT)

8.1.1 Introduction

The Incident Management System (IMS) Application Configuration Tool (ACT) provides a graphical user interface to configure the static information in the IMS PDA Application. The tool allows you to configure:

- Sector / Division information,
- Incident Type information, and
- PDA User Profiles.

A **Sector/Division** is a physical area or activity assignment that occurs during an incident. A sector might be Sector A or Roof at a fire to which an asset or resource is assigned. A division might be HazMat at a hazardous materials incident. During an incident, assets (fire fighters, law enforcement personnel, or EMS vehicles or equipment) are assigned to a Sector/Division.

An **Incident Type** is how the incident is described, such as a Structure Fire, Hostage Situation, or Motor Vehicle Accident. When an incident is started on the PDA, the Incident Commander (IC) has an opportunity to select an incident type.

A **PDA User Profile** includes basic information about the PDA user, such as their User ID, authentication code, common name, and their jurisdiction. When a PDA user logs into the PDA to start an incident, their profile will determine how they log in and what data appears on the PDA screen and in the incident log.

Lists of standard sectors/divisions, incident types, and user profiles are pre-loaded in the ACT. These lists are also available for download in MS Word format from the TeraHop Customer Resource Management (CRM) tool. See Warranty Service and Technical Support.

To get started, please go to the following:

IMS Application Assignment Labels and Types

How to Configure the IMS PDA Application

8.1.2 IMS Application Assignment Labels and Types

The following matrix indicates the Master List of Assignment-label/type choices that are available for configuration into the IMS application for use by PDAs and Incident Status Board (ISB). The choices are configured into the IMS application using the ADMS and the Application Configuration Tool (ACT). A user/agency is free to select from this matrix which Assignment labels will be presented to the IC in the Make Assignment list when he wants to assign an asset to a task or function. The ISB automatically follows the labels used by the PDA.

This matrix also indicates the default settings for three types of usage: Mixed, Fire, and Law Enforcement. The user/agency may simply opt to use one of the defaults, may modify one of the defaults and use it, or may design his own list from the Master List.

The user should note that some of the Assignment labels are required in all/any configurations. The user will also note that, due to the different natures of the PDA and the ISB, some assignments appear on the PDA and not on the ISB, and vice-versa.

Table 4: Assignment Labels/Types

			Default Mixed	**Default Fire**	**Default Law Enforcement**		
Assignment Type	**Master List of Assignment Labels**	**Default Hot Zone**	**On PDA**	**On PDA**	**On PDA**	**Agency Emphasis**	**Explanation**
Functional/Org.							
	Incident Cmd.					all	Incident Command
	Ops		x	x	x	all	Operations
	Logistics		x	x	x	all	Support
	Planning		x	x	x	all	
	Comm./Scribe		x	x	x	all	
	Finance		x	x	x	all	
	Info/Liais.		x	x	x	all	Information and liaison
	Safety		x	x	x	all	
Task/Location							
	Div. A		x		x	all	address or main-entrance side of structure/site
	Div. B		x		x	all	clockwise one side from A side
	Div. C		x		x	all	clockwise one side from B side
	Div. D		x		x	all	clockwise one side from C side
	Exp. A	x		x		fire	address or main-entrance side of structure/site

			Default Mixed	Default Fire	Default Law Enforcement		
Assignment Type	**Master List of Assignment Labels**	**Default Hot Zone**	**On PDA**	**On PDA**	**On PDA**	**Agency Emphasis**	**Explanation**
	Exp. B	x		x		fire	clockwise one side from A side
	Exp. C	x		x		fire	clockwise one side from B side
	Exp. D	x		x		fire	clockwise one side from C side
	Air Ops		x	x	x	all	landing and support areas for aircraft
	Assault	x			x	law enforcement	
	Backup				x	law enforcement	
	Barricade					PW	
	Basement	x	x	x	x	fire	
	Bomb/Exp	x			x	law enforcement	
	Contain		x			hazmat	
	Crowd		x		x	law enforcement	crowd control
	Debris		x			PW	clearing debris (e.g., sawing blocking trees)
	Decon	x				hazmat	
	EMS/Med.		x	x	x	med.	generic medical
	Entry/Lobby	x	x	x	x	fire	at the main entrance of a building
	Evac.		x	x		fire	getting victims out/away from affected area
	Extricate	x				fire	
	Fire Attack	x	x	x		fire	
	Hazmat		x	x		fire	generic Hazmat activities
	Hostage/HNT				x	law enforcement	
	Hot Zone	x				hazmat	a particular

			Default Mixed	**Default Fire**	**Default Law Enforcement**		
Assignment Type	**Master List of Assignment Labels**	**Default Hot Zone**	**On PDA**	**On PDA**	**On PDA**	**Agency Emphasis**	**Explanation**
							Hazmat zone
	Interior	x	x	x	x	fire	all interior, except as noted elsewhere
	Investigation		x	x	x	law enforcement	may include arson and PW inspections
	Lighting			x			
	Main Floor	x	x	x	x	fire	
	Marine Ops						riverine, lake, shoreline, etc.
	Overhaul			x		fire	
	Perimeter		x	x	x	law enforcement	control of site access
	Pumping					PW	removal of standing fluids
	Rescue	x	x	x	x	fire	recovery of victims in distress
	Rehab		x	x	x	all	rest area and replenishment of air packs
	RIT			x		fire	Rapid Intervention Team
	Roof	x	x	x	x	fire	
	Road/Brdg.		x			PW	all activities related to roads and bridges
	Salvage		x	x		fire	
	Search	x	x	x	x	fire	initial and subsequent searches for people inside
	Shoring		x			PW	strengthening of structures & barriers (e.g., levies)
	Sniper	x			x	law enforcement	
	Staging		x	x	x	all	where assets are usually sent prior to being given 1st assignment
	Stairs	x	x	x		fire	a specific interior

			Default Mixed	**Default Fire**	**Default Law Enforcement**		
Assignment Type	**Master List of Assignment Labels**	**Default Hot Zone**	**On PDA**	**On PDA**	**On PDA**	**Agency Emphasis**	**Explanation**
							assignment
	Strike Team	x			x	law enforcement	
	Suppression		x	x		fire	
	Triage		x			med.	
	Treatment		x			med.	
	Traffic		x	x	x	law enforcement	traffic control
	Transport		x			med.	
	Upper Floor	x	x	x	x	fire	
	Utilities		x	x		PW	power, gas, phone, street lights. sanitation, water system
	Ventilation	x	x	x		fire	
	Warm Zone					Hazmat	a particular Hazmat zone
	Water Supply		x	x		fire	finding and connecting to a water source
	Other		x	x	x	all	any/all other not listed
Special							
	Released		x	x	x	all	assets that have been released from incident but which may still be on scene.
	To Unit		x	x	x	all	a label that, when clicked, presents a list of units that are present at that incident, to which an asset may be assigned.
	New/Add		x	x	x	all	a label that, when clicked, opens a tool to add an assignment type to the list available for that incident.
Total Counts	68		47	42	37		Max capacity of ISB = 46

Notes:

The items in the Master List of Assignment Labels column, except for Other, Released, To Unit, and New/Add, are available in the Application Configuration Tool (ACT) for you to select for use in the system. Or, you can use one of the three defined defaults. Or, you can select a default and modify it.

Other, Released, To Unit, and New/Add are always in the PDA and ISB, as indicated. The items in this column are also available for auto-suggest if the IC uses the uses the New/Add feature on the PDA.

8.1.3 How to Configure the IMS Application

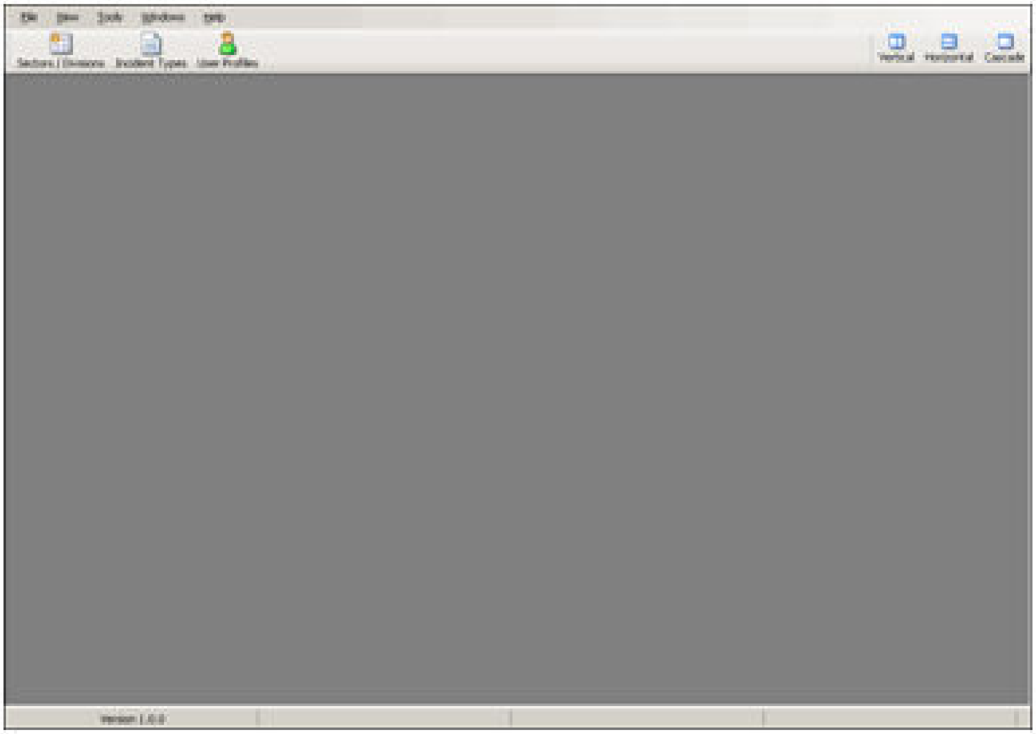
The following paragraphs describe how to enter data that will appear on the IMS Application PDA screen, including sectors/divisions, incident types and user profiles.

8.1.3.1 Getting Started

Before you begin, do the following:

Plug the Ethernet cable from the laptop computer running the ACT into the same Ethernet switch that the MMR is plugged into. In this manner, the ACT can access the Domain Name Server that is located in the MMR which will give it the proper IP Address needed to operate with the IMS system.

To use the program, double-click the **IMS ACT** icon on the desktop. IMS ACT
The **IMS Application Configuration** screen appears displaying three icons in the second toolbar. **Note:** these three functions are also available from the **Tools** menu in the top toolbar.



The icons described below provide access to the configurable information so that you can enter, delete, or update it.

Sectors / Divisions

The **Sector/Divisions** icon enables you to manage the configured sector/division information in the system. The Sector/Division list appears on the PDA so that the user can assign an asset to a sector/division.

Incident Types

The **Incident Types** icon enables you to manage the configured incident types in the system. The Incident Type list appears on the PDA when the user is creating the incident.

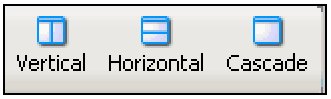
User Profiles

The **User Profile** icon enables you to manage the configured User Profile information in the system. The User Profile data is used to authenticate the PDA users when they log in.

8.1.3.2 Configuration Tool Window Display Management

When you click one of the three program icons illustrated above, it opens a form in a new window. Several forms may be open simultaneously.

You can manage how the screen displays these forms in Windows using the **Vertical, Horizontal**, or **Cascade** icons that are located in the upper right corner of the screen (see below).



Vertical will arrange all of the open forms in a vertical fashion.

Horizontal will arrange all of the open forms in a horizontal fashion.

Cascade will arrange all of the open forms in a cascaded fashion.

Continue to the following topics:

How to Configure Sectors/Divisions for the PDA

How to Configure Incident Types for the PDA

How to Configure User Profiles for the PDA

8.1.4 How to Configure Sectors/Divisions for the IMS Application

Adding, deleting, and updating records works the same throughout the ACT whether you are configuring sectors/divisions, incident types, or user profiles.

The table below describes the icons used to perform these functions. After you select to manage incident types, user profiles, or sectors/divisions, these icons are available.

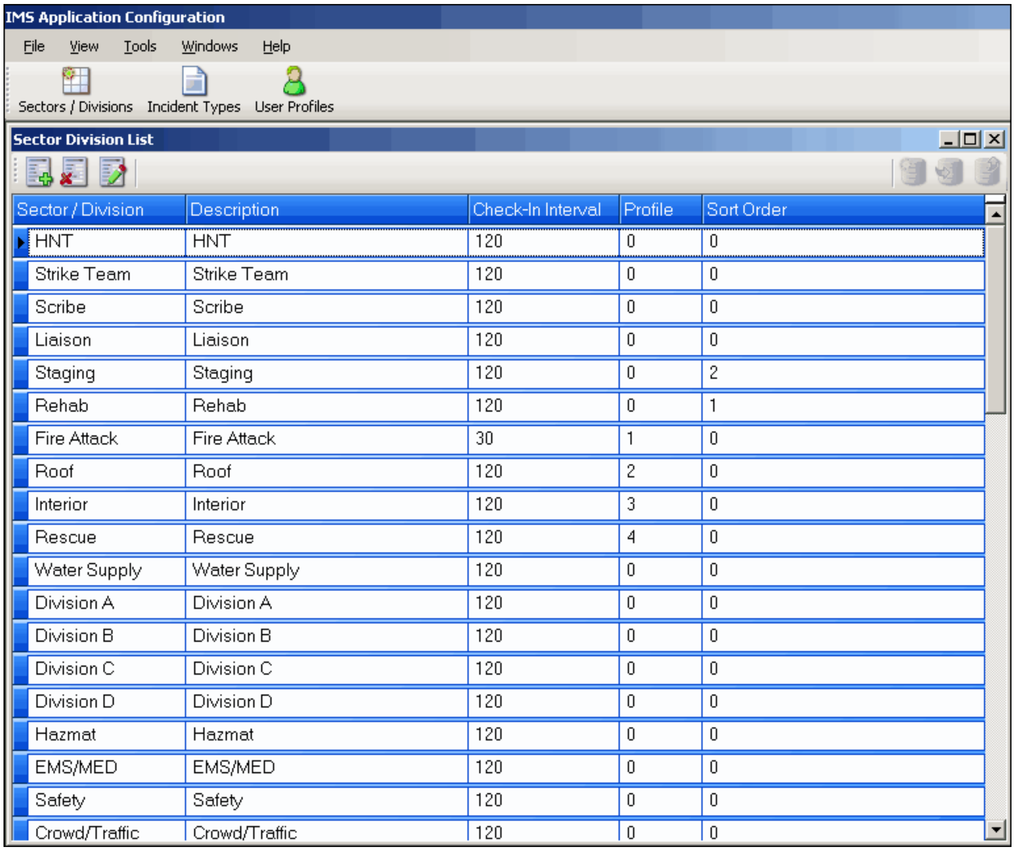
Table 5: IMS ACT Record Management Icons

Add	Click this icon to enter a new record for a selected function, such as a sector/division.
Delete	Click this icon to delete a record for a selected record in the table.
Update	Click this icon to display and update the contents of the currently selected record.

The following paragraphs describe how to configure sectors/divisions that will appear on the IMS screen during an incident.

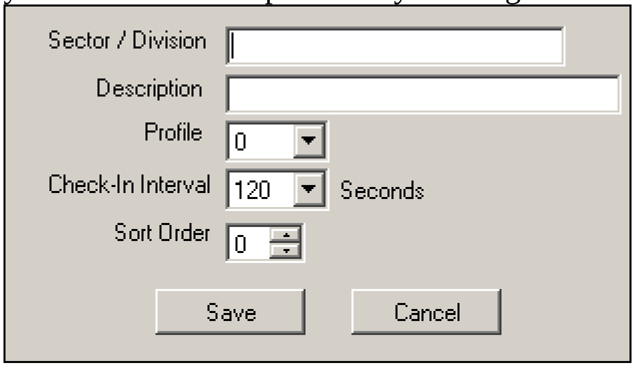
To configure sectors/divisions, do the following:

1. Click the **Sectors/Divisions** icon.
The **Sector Division List** screen appears displaying the rows and columns for data to enter for each record in the sector/division database. The application table shown below is pre-populated with default values. These defaults can be used, edited, or deleted using this table.



Sector / Division	Description	Check-In Interval	Profile	Sort Order
HNT	HNT	120	0	0
Strike Team	Strike Team	120	0	0
Scribe	Scribe	120	0	0
Liaison	Liaison	120	0	0
Staging	Staging	120	0	2
Rehab	Rehab	120	0	1
Fire Attack	Fire Attack	30	1	0
Roof	Roof	120	2	0
Interior	Interior	120	3	0
Rescue	Rescue	120	4	0
Water Supply	Water Supply	120	0	0
Division A	Division A	120	0	0
Division B	Division B	120	0	0
Division C	Division C	120	0	0
Division D	Division D	120	0	0
Hazmat	Hazmat	120	0	0
EMS/MED	EMS/MED	120	0	0
Safety	Safety	120	0	0
Crowd/Traffic	Crowd/Traffic	120	0	0

8. To add a new record to the database, click **Add.**
The **Sector/Division Details** dialog box opens. **Note:** At any time during this process, you can cancel the operation by clicking **Cancel**.



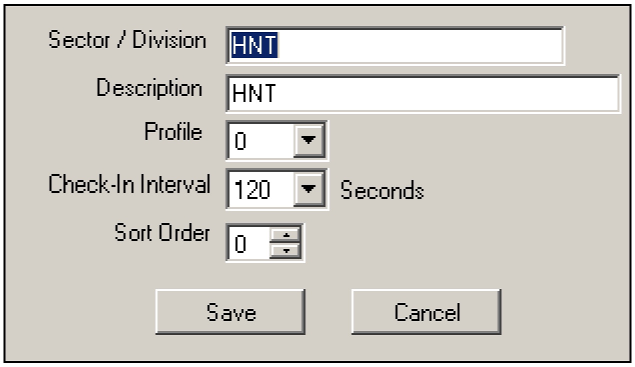
Sector / Division
Description
Profile 0
Check-In Interval 120 Seconds
Sort Order 0

9. Complete the fields in the dialog box using the information in the table below, and click **Save**.
   The new record will appear in the **Sector Division List**.

Field	Data to Enter
Sector/Division	The name of the sector or division as you want it to appear on the IMS display.
Description	A brief description of the sector or division.
Profile	The number of the profile that has been configured in the RSN profile for this sector/division.
Check-in Interval	The amount of time, in seconds, that equals the check-in value in the profile specifics.
Sort Order	The order in which you want this sector/division to appear on the PDA display.

Important!
It is critical that the profile and check-in interval be entered with the same values as those in the RSN Configuration Tool (RCT). If different values are entered, the system may fail to operate properly.

10. To update a record, double-click to open the record or select the record and click the **Update** icon, make your changes, and click **Save**.

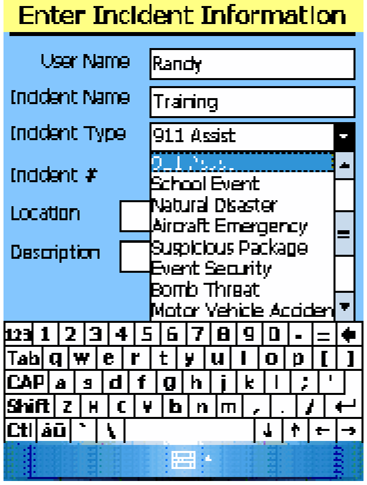


Sector / Division: HNT
Description: HNT
Profile: 0
Check-In Interval: 120 Seconds
Sort Order: 0

11. To delete a record, select the record and click the **Delete** icon.
    The following message appears: *Are you sure you want to delete xxx?*
12. To cancel the delete, click **Cancel**.
13. To delete the record, click **Yes**.
    The record is deleted.

8.1.5 How to Configure Incident Types for the Application

The following paragraphs describe how to configure incident types that are selectable from the IMS PDA during an incident. When the Incident Commander begins an incident in the PDA, incident types appear in the **Incident Type** drop-down list on the **Enter Incident Information** screen on the PDA, as shown below.



Enter Incident Information

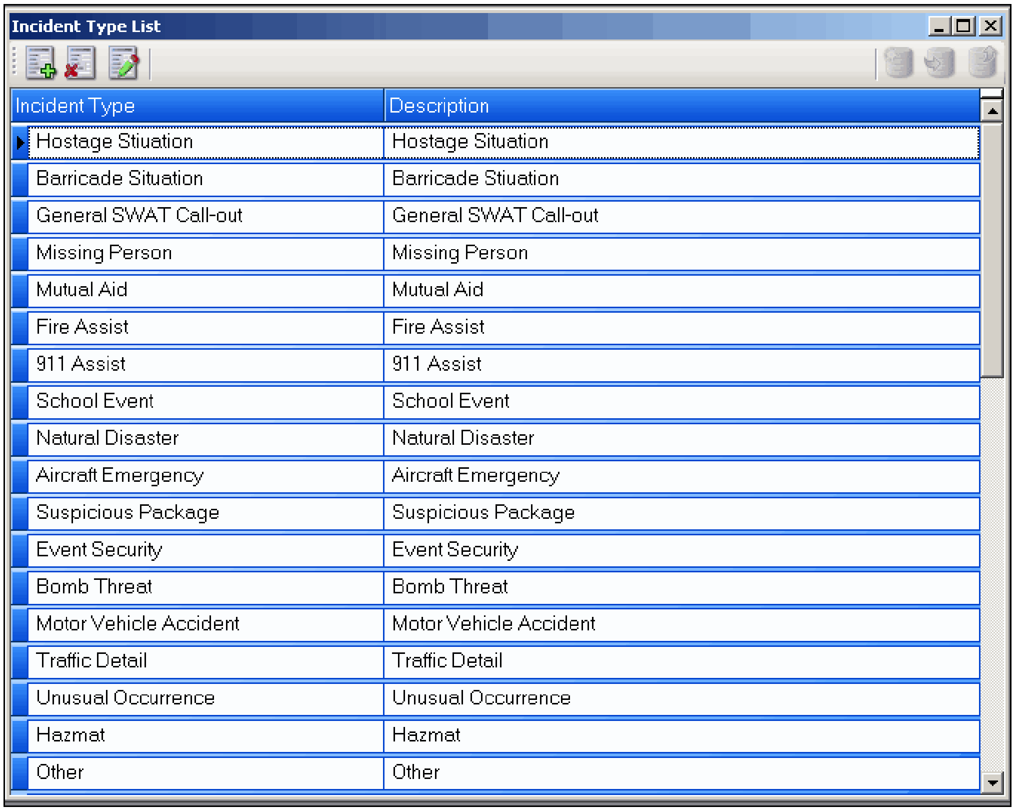
User Name: Randy

Incident Name: Training

Incident Type: 911 Assist

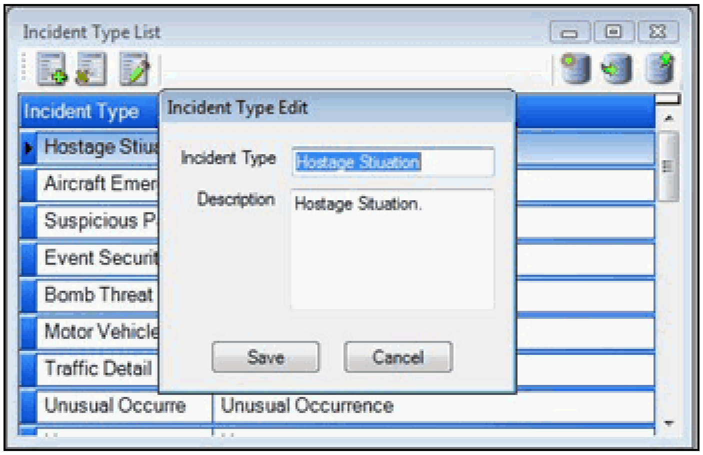
To configure incident types, do the following:

1. Click the **Incident Types** icon. Incident Types
   The **Incident Type List** screen appears displaying a list of default incident types. The descriptions shown below are samples. The description can be anything the user wants it to be.



Incident Type	Description
Hostage Stiuation	Hostage Situation
Barricade Situation	Barricade Stiuation
General SWAT Call-out	General SWAT Call-out
Missing Person	Missing Person
Mutual Aid	Mutual Aid
Fire Assist	Fire Assist
911 Assist	911 Assist
School Event	School Event
Natural Disaster	Natural Disaster
Aircraft Emergency	Aircraft Emergency
Suspicious Package	Suspicious Package
Event Security	Event Security
Bomb Threat	Bomb Threat
Motor Vehicle Accident	Motor Vehicle Accident
Traffic Detail	Traffic Detail
Unusual Occurrence	Unusual Occurrence
Hazmat	Hazmat
Other	Other

2. To add a new record to the database, click **Add.**
   The **Incident Type** dialog box opens. In this example, the Hostage Situation incident type is being added. **Note:** At any time during this process, you can cancel the operation by clicking the **Cancel** button.



Hostage Stiu
Aircraft Emer
Suspicious P
Event Securit
Bomb Threat
Motor Vehicle
Traffic Detail
Unusual Occurre | Unusual Occurrence

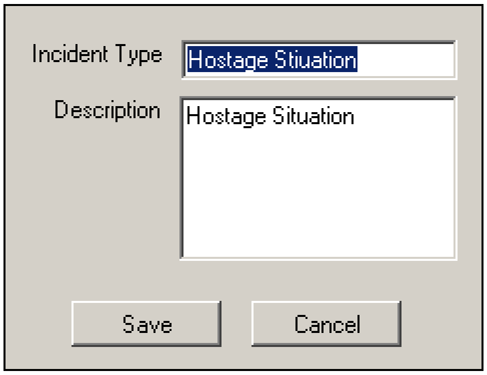
Incident Type: Hostage Stiuation

Description: Hostage Situation.

3. Complete the fields in the dialog box using the information described in the table below, and click **Save**.
   The new record will appear in the **Incident Type List**.

Field	Data to Enter
Incident Type	The name of the incident type to appear on the PDA display.
Description	A brief description of the type of incident.

14. To update a record, double-click to open the record or select the record and click the **Update** icon, make your changes, and click **Save**.



Incident Type: Hostage Stiuation

Description: Hostage Situation

15. To delete a record, select the record and click the **Delete** icon.
    The following message appears: *Are you sure you want to delete xxx?*

16. To cancel the delete, click **Cancel**.

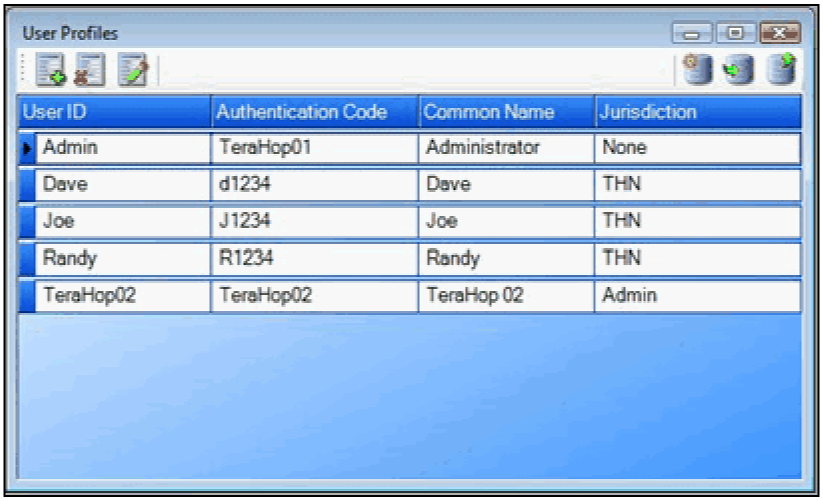
17. To delete the record, click **Yes**.
    The record is deleted.

8.1.6 How to Configure User Profiles for the IMS Application

The following paragraphs describe how to configure user profiles that define users of the IMS Application.

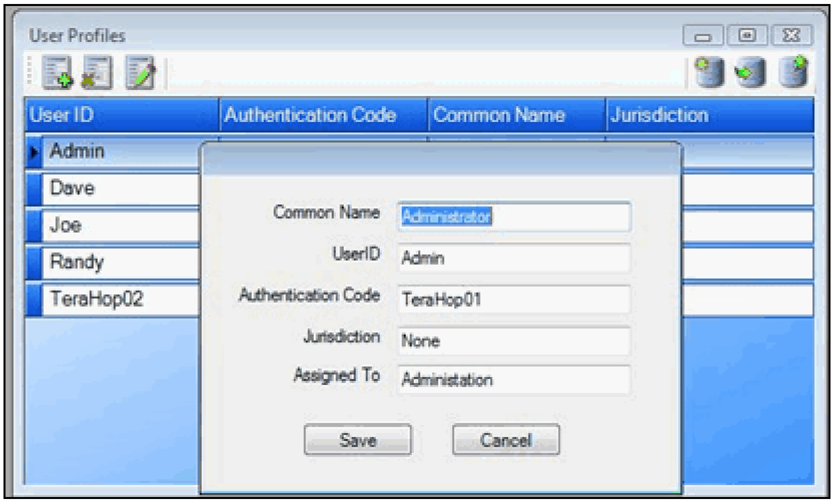
To configure user profiles, do the following:

1. Click the **User Profiles** icon.
   The **User Profiles** screen appears displaying the rows and columns for data to enter for each record in the user profiles database.
   Note: The default user IDs are: User ID, **Admin**; Authorization Code, **Password**.



User ID	Authentication Code	Common Name	Jurisdiction
Admin	TeraHop01	Administrator	None
Dave	d1234	Dave	THN
Joe	J1234	Joe	THN
Randy	R1234	Randy	THN
TeraHop02	TeraHop02	TeraHop 02	Admin

2. To add a new record to the database, click **Add.**
   The **User Profile** dialog box opens. In this example, the Administrator user profile is being added. **Note:** At any time during this process, you can cancel the operation by clicking the **Cancel** button.



Common Name: Administrator

UserID: Admin

Authentication Code: TeraHop01

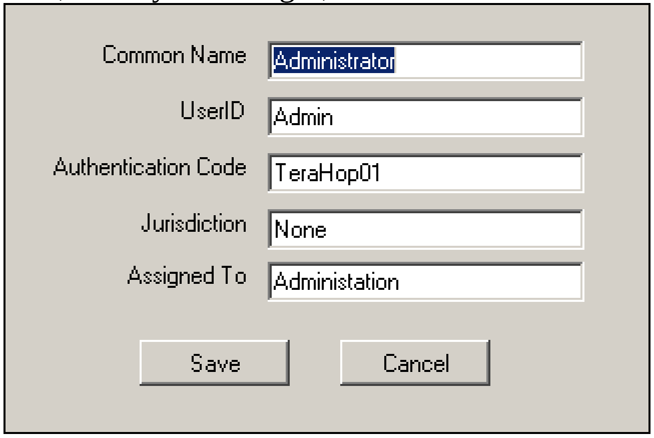
Jurisdiction: None

Assigned To: Administation

3. Complete the fields in the dialog box using the information described in the table below, and click **Save**.
   The new record will appear in the **User Profiles** screen.

Field	Data to Enter
Common Name	The person's real name, such as John Smith or their role such as Administrator or Incident Commander.
User ID	The ID to appear on the PDA display and in the incident logs. **Note:** The default User ID is Admin.
Authentication Code	The code this person needs to enter to log into the PDA. Codes can be all numbers, all letters, or alphanumeric. Codes are not case sensitive. Codes must be 3 to 32 characters long. **Note:** The default authentication code is Password.
Jurisdiction	The jurisdiction to which this person belongs, such as the county or department to which the person reports. Jurisdictions can be 64 characters long.
Assigned to	This field is user definable. It can be what the administrator wants it to be. For example, an administrator may be assigned to Administrator, but a Battalion Chief might be assigned to Station 35.

18. To edit a record, double-click to open the record or select the record and click the **Update** icon, make your changes, and click **Save**.



Common Name	Administrator
UserID	Admin
Authentication Code	TeraHop01
Jurisdiction	None
Assigned To	Administation

19. To delete a record, select the record and click the **Delete** icon.
    The following message appears: *Are you sure you want to delete xxx?*

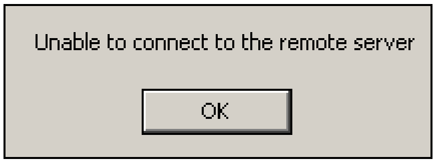
20. To cancel the delete, click **Cancel**.

21. To delete the record, click **Yes**.
    The record is deleted.

8.1.7 IMS Application Configuration Tool (ACT) Error Conditions

All of the data entered is edit checked prior to adding it to the database. If a field does not meet the validation criteria, a message box appears to inform you of the error and the cursor is placed in the field that is in error.

When entering data in the ACT, if the software is unable to connect to the IMS Application PDA Server, a message appears indicating that the software could not connect to the service and no data will be displayed in the list. Make sure that you have plugged the Ethernet cable from the Laptop running the Application Configuration Tool into the same Ethernet switch that the MMR is plugged into. In this manner, the Application Configuration Tool can access the Domain Name Server that is located in the MMR which will give it the proper IP Address needed to operate with the IMS system.



Unable to connect to the remote server

8.2 Configuring RSNs with the RSN Configuration Tool (RCT)

8.2.1 Introduction

The TeraHop Networks (THN) Remote Sensor Node is an intelligent wireless device which can be programmatically configured to perform and behave in a predetermined manner in the field. This RSN Configuration Tool (RCT) instructions section (see Using the RCT) is intended to provide detailed instructions on how to create and/or edit all types of configurations, download configurations into RSNs, and manage the created configurations in order to define the RSN's field performance and behavior.

For specific instructions on configuring RSNs for the TeraHop Incident Management System (IMS) *with* Automated Accountability application for First Responders, see Configuring RSNs for the IMS.

Application Users

Users of this tool will be personnel of any company who will configure the parameter settings within the RSN which will govern the performance and behavior characteristics of RSNs as they encounter conditions in the field. In addition, Advanced users will be supported to configure more advanced behavior and network interface capabilities of the RSNs as well as manage the administrative duties of the application.

The individuals using the Tool should have at least an associate-level degree in electronics and/or IT, and be familiar with wireless data networking.

RCT Users

There are two levels of roles for users of the RCT: the **User** role and the **Advanced** role, controlled through user authentication at the time of log-in.

The User role has a limited set of the Advanced role's functionality as they do not have access to Advanced role's settings.

The Advanced role has all the capabilities of the User role plus administrative rights to set advanced configurations and administer user accounts.

Definition of Terms

Mobile Gateway Administration Station (ADMS) is a software administrative platform in which several applications reside and is used in managing the components of the TeraHop network. Integral capabilities of this platform include the ability to:

- Manage customer applications
- Access network data
- Maintain and update network components
- Run network component configuration applications
- Obtain system logs

An illustration of this capability is shown below.

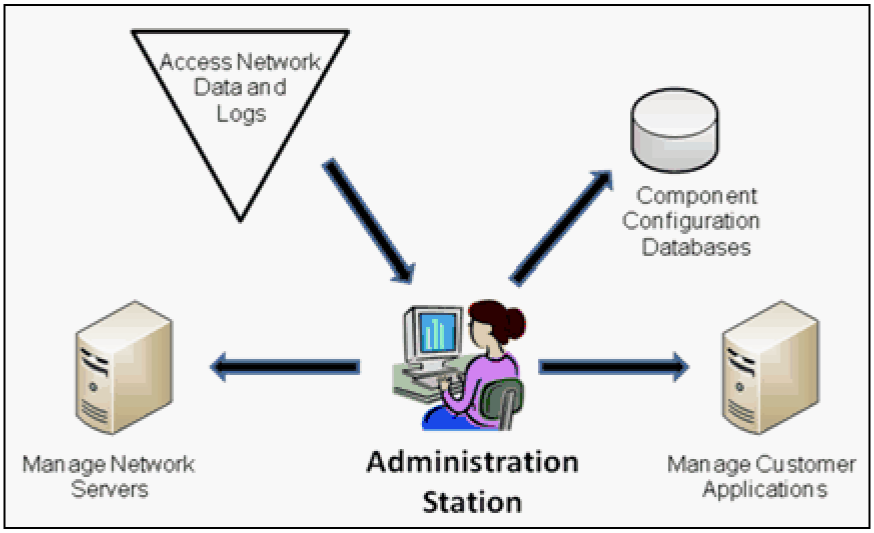

Access Network Data and Logs
Component Configuration Databases
Manage Network Servers
Administration Station
Manage Customer Applications

Figure 14: Mobile Gateway Administration Station (ADMS)

8.2.2 TeraHop Console

The THC is a software framework from which tools are selected. The console is a framework for the management and access of network and application utilities. User administrative rights and user authentications are controlled from within the Console. Applications are installed and managed within the TeraHop Console as “add-ins.”

Applications that currently reside from within the Console include the RSN Configuration Tool (RCT), the TeraHop Data Extraction Tool (TDX), and the RSN Configuration Viewer (RCV). Additional administrative applications will be added as they become available.

The RSN Configuration Tool (RCT) is an application that resides within the TeraHop Console (THC) on the Administration Station (ADMS) laptop computer. The RCT is used to define and download the capabilities and processes that manage the functionality and behavior of the Remote Sensor Nodes (RSNs) as they encounter conditions in the field.

The main purpose of the RCT is to configure the behaviors of each RSN. Configurations are a full set of programmable RSN parameters including network management, behavior profiles, and user data. To do this, two main areas within the ACT require configuration: the configuration tree and the RSN. In addition, each RSN is shipped with a default configuration. Each of these is defined further below.

- Factory Configuration (THN provided) contains the configuration parameters that the RSN is shipped with when it arrives from the factory. The RSN will behave according to these parameters unless configured otherwise: All sensors are turned off, No User Data, and No behavior parameters.

- Default Configuration is a configuration provided by TeraHop Networks in the RCT and cannot be edited by users or administrators. All other configurations are derived from this configuration. This is the top level in the configuration tree.
- RSN Configurations are specific configurations that associate an RSN with a specific configuration and allows user data to be customized for that RSN.
- ClassID is a group of identifiers that help define the network with which an RSN is able to communicate.
- Behavior Profiles define the behavior of the RSN as it encounters situations in the field. The Tool is provided with default behaviors that will define the behavior of the RSN unless changed. The behaviors are broken into several categories or sensors (each sensor has its own tabbed section broken down by functionality) to assist you in changing only those parameters that are required.
- Sensors Each RSN is equipped with a motion and shock sensor that can be enabled and configured with the Tool. The default configuration is to have the sensors disabled. Parameters that can be configured include the sensitivity of each sensor, the frequency of the sensor alarm, and the duration of an event that must take place prior to the sensor alarm being activated.
- Inheritance The Tool uses a concept called Inheritance, whereas the parameters are automatically inherited from a configuration of a higher level, unless specifically edited. The inheritance dependencies are defined prior to defining any specific RSN configurations. This approach allows you to easily and quickly configure like assets without having to re-enter a full configuration for each.

8.2.3 RSN Configuration Overview

RSNs are wireless electronic devices. They are one of the three key network elements of the movable wireless sensor network offered by TeraHop Networks. The behavior of these devices provides the core functionality on how the assets associated with an RSN within the network will be monitored and managed. The RSNs also affect many of the network communication behaviors and provide vital data to the network concerning each asset.

The identified applications for the RSN require specific RSN functionality that is to be defined at the market level and configured within the supported RSNs. For example, the First Responder market may require different sensor settings and network check-in rates depending on the on-scene incident assignments.

RSNs have a set of features that are intended to enable the use of a single basic design across several applications. The types of events/conditions that applications typically need to monitor or react to, for which all RSNs need to be equipped to support, include:

- RSN Presence – RSN detects and reports that it is in range of and accepted by an appropriate TeraHop network.

- RSN Movement – RSN detects and reports that it has begun to move, stopped moving, or has not moved (depending on the application) for some period of time (set by you).
- RSN Shock – RSN detects and reports a shock that exceeds some pre-programmed threshold.

Depending on the application, the RSN will be used to dictate the behavioral requirements of each device. It is through the configuring of the RSN through the RSN Configuration Tool that these behaviors are defined.

Each RSN configuration has approximately 70 parameters that can be set. All settings have factory defaults established that may or may not require editing based on your system. In addition, depending on your access rights to the application, not all parameters may be available to you. Some parameters are intended to be managed by a technical administrator (Advanced role) with network experience, while others are intended for general configuration purposes (User role).

Behavior Profiles are set within each RSN that define how the RSN will behave under specified field conditions or from commands from a user application. Throughout this section, we will be referencing the First Responder application as an example.

8.2.4 The RCT Configuration Inheritance

The RCT manages all of the configurations that are required to define the behavior of an RSN. Configurations are organized in an inheritance structure with lower levels deriving settings and behaviors from higher levels. The structure is similar to that of a waterfall, whereas, data from the upper level configurations cascades down to those below it. Each lower configuration takes on the behaviors of the upper configurations unless specifically changed within the Configuration Tool.

Depending on the application, the assets may need one or many configurations to handle the behavior desired of their RSNs. The RCT allows the user to create a database of many configurations and assign the RSNs to use the applicable configurations. This is achieved by defining and setting up all of the needed configurations for the defined set of RSNs and then associating each RSN with the configurations through an assigning process.

As mentioned previously, configurations are organized into a tree (inheritance) structure. The application is provided with one-top level default configuration. For the IMS with Automated Accountability application, all configurations should derive from the First Responder market configuration. All inherited configurations are derived from this one top-level default configuration. All default settings can be changed in subsequent lower levels. The default values are provided by THN at the time of delivery to provide the basic behaviors for each configuration.

When creating a new configuration, its parameter settings are derived from the top-level default settings until those settings are individually overridden. You may derive all of an RSN's configurations from the top level or you may derive your own configurations, thus creating a library of configurations. Each setting has an inheritance control that allows you to override the default.

Configuration Process Overview

One of the keys to successfully configuring RSNs through the use of the RCT is to pre-plan the RSN configuration structure. This should be completed prior to creating any configurations within the Tool.

With the ability to create a tree (inheritance) structure of configurations (remember the waterfall analogy where the lower configurations are determined by those above them), it is worth taking some time to consider how you would structure the configuration in order to minimize the number of configurations for each RSN.

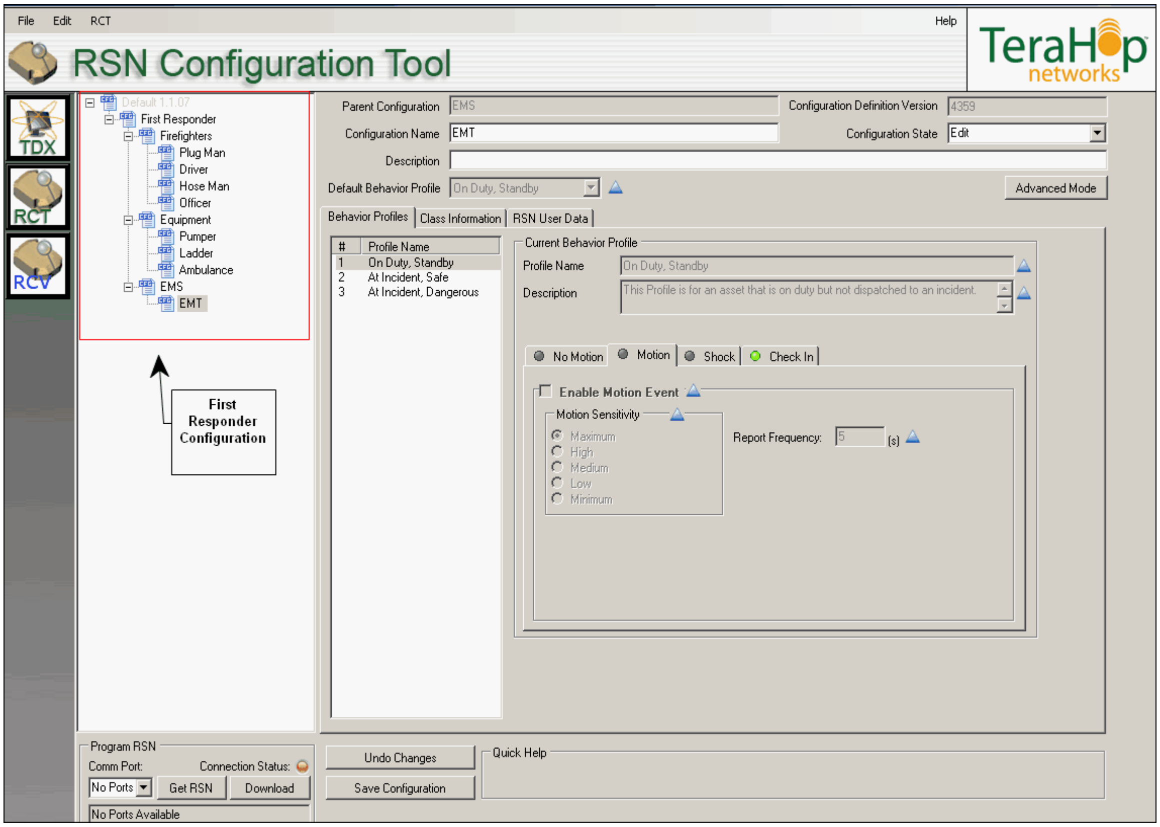
The goal is to create an organization tree that best uses the settings of the upper level configurations for those that are below it. For instance, configurations between persons and equipment may be different enough that two configurations may be desired at an upper level, one for persons and the other for equipment.

To assist in this process, it would be worthwhile asking the following questions:

1. How can assets be organized into similar groups, such as persons or equipment?
2. How do the RSNs need to behave? List them out and make note of the differences and similarities.
3. How can these differences and similarities be organized into some type of structure?
4. How can I take advantage of the inheritance organization?

The key to consider here is to determine where there are higher-level configurations where one setting can be controlled from that level and be passed down to the lower levels.

The following example shows how a typical First Responder configuration may be set up. The left-hand panel is always where configurations and RSN assignments are defined.



- Default 1.1.07
  - First Responder
    - Firefighters
      - Plug Man
      - Driver
      - Hose Man
      - Officer
    - Equipment
      - Pumper
      - Ladder
      - Ambulance
    - EMS
      - EMT

Parent Configuration: EMS

Configuration Definition Version: 4359

Configuration Name: EMT

Configuration State: Edit

Description:

Default Behavior Profile: On Duty, Standby

#	Profile Name
1	On Duty, Standby
2	At Incident, Safe
3	At Incident, Dangerous

Profile Name: On Duty, Standby

Description: This Profile is for an asset that is on duty but not dispatched to an incident.

□ Enable Motion Event

● Maximum

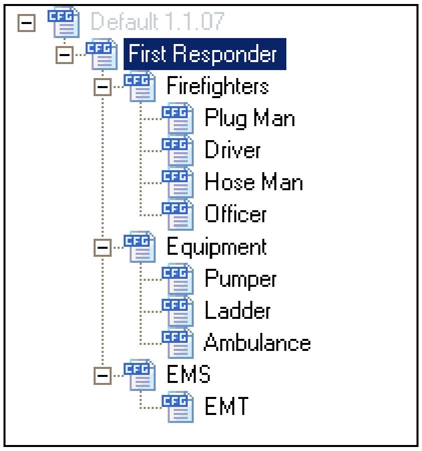
Report Frequency: 5 [s]

Comm Port: No Ports

Connection Status:

No Ports Available

Once the planned configuration tree structure is designed, create it in the RCT (details on how to accomplish this are defined later in the instructions). You will then go to each configuration level and select the appropriate parameters and settings to be associated with the corresponding configuration.



- Default 1.1.07
  - First Responder
    - Firefighters
      - Plug Man
      - Driver
      - Hose Man
      - Officer
    - Equipment
      - Pumper
      - Ladder
      - Ambulance
    - EMS
      - EMT

8.2.5 Installing the RCT

The RCT is an add-in on the TeraHop Console (THC) and is pre-loaded on the ADMS laptop computer. If you should need to install the RCT, please contact TeraHop Networks Customer Service.

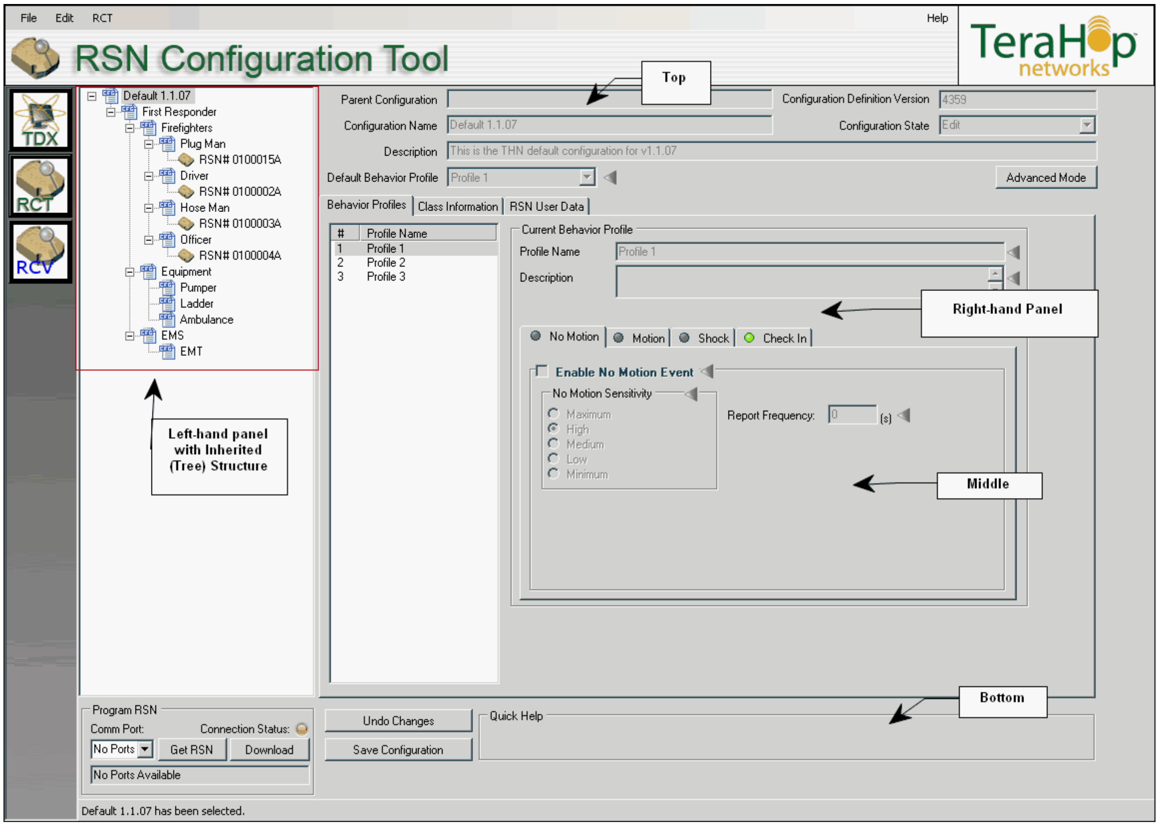
8.2.6 Using the RCT

The RCT is accessed from the TeraHop Console (THC) on the TeraHop Administration Station (ADMS). For instructions on logging into and using the THC, go to Working with the TeraHop Console and Its Applications in this manual. Once you log into the THC, you do not need to log into the RCT. You can just open the application by clicking on the RCT icon on the left-hand panel.

To start the RCT, do the following:

From the THC on the ADMS laptop computer, click the **RCT** icon.

Upon opening the application, notice that the RCT application is laid out such that the left-hand panel displays the configuration tree, while the right-hand panel shows the selected configuration settings.



Default 1.1.07
- First Responder
  - Firefighters
    - Plug Man
      - RSN# 0100015A
    - Driver
      - RSN# 0100002A
    - Hose Man
      - RSN# 0100003A
    - Officer
      - RSN# 0100004A
  - Equipment
    - Pumper
    - Ladder
    - Ambulance
  - EMS
    - EMT

Parent Configuration:
Configuration Name: Default 1.1.07
Description: This is the THN default configuration for v1.1.07
Default Behavior Profile: Profile 1
Configuration Definition Version: 4359
Configuration State: Edit

#	Profile Name
1	Profile 1
2	Profile 2
3	Profile 3

Current Behavior Profile
Profile Name: Profile 1
Description:

□ Enable No Motion Event
No Motion Sensitivity
○ Maximum
● High
○ Medium
○ Low
○ Minimum
Report Frequency: 0 (s)

Program RSN
Comm Port: No Ports
Connection Status:
No Ports Available

Default 1.1.07 has been selected.

The following paragraphs describe each panel in more detail.

Left-hand Panel

This panel shows all of the configurations in their inherited (tree) structure, from the top-level default configuration down to the RSN configurations.

This view allows you to select a specific configuration to be used when configuring a specific type of RSN(s).

Select an item from the left-hand panel. All of the settings for that selection are loaded into the right-hand panel. In the illustration above, the selection of Plug Man will cause all of the behavior settings for the Plug Man to be pre-loaded in the right-hand panel.

Right-hand Panel

This panel serves as an editor to define the parameters for the currently selected left-hand configuration (see left-hand panel above). There are approximately 70 parameters that can be configured for each RSN in this section.

This section of the application is broken into three additional sections referred to as the Top, Middle, and Bottom. Each section provides unique and pertinent information for the overall behavior and settings for the selected left-hand configuration.

In the Top Section, you can edit general information about the selected configuration such as its name, description and the default behavior profile associated with the selected left-hand panel configuration.

The Middle section is broken down into several tabs with each tab supporting the editing of specific types of configuration data. The following parameters are supported in this section:

- Behavior Profiles
- Class Information
- RSN User Data
- Configure User Data (Advanced mode only)
- In addition, the Current Behavior Profile section has several tabs to define specific behavior characteristics for the selected configuration. These tabs include:
- No Motion
- Motion
- Shock
- Check-in

The Bottom of the middle section provides you with controls to manage the editing of the configurations and supports such functions as:

- Undo Changes
- Save Configuration

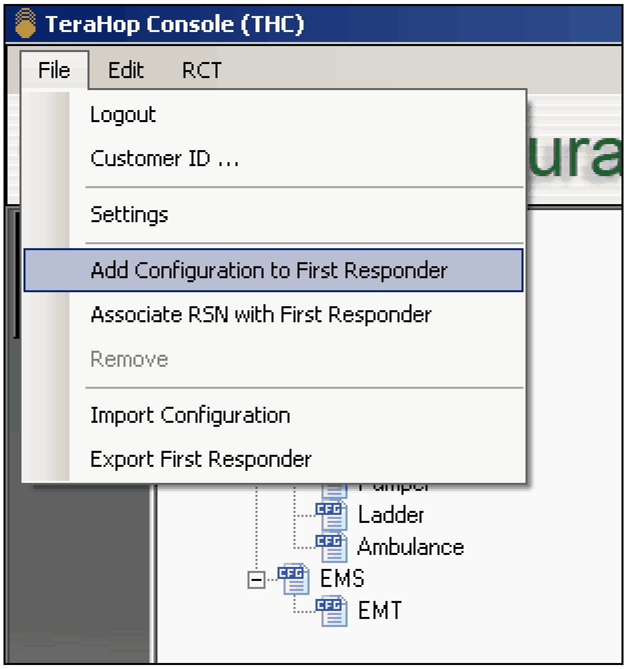
This section also provides you with a Quick Help window which displays a brief description of the selected parameter along with helpful hints on the setting currently in focus. (Hint: You can click on any setting control to get the Quick Help for that setting. If the control is read only, then click on its adjacent inheritance control.

8.2.7 Creating a Left-Hand Configuration Tree in the RCT

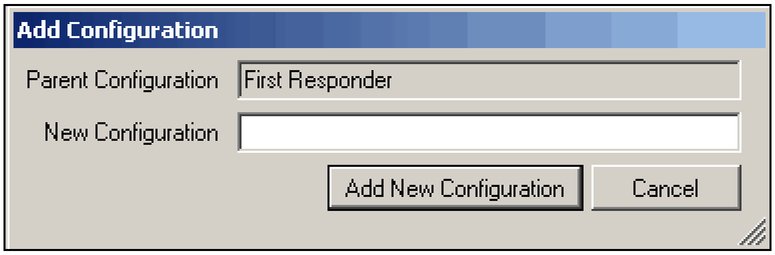
In the Left-hand panel, the application comes provided with a default configuration. Market-specific configurations may also be provided based on the application.

To create additional configurations under these market-specific configurations, do one of the following, as shown in our First Responder example:

1. In the left-hand panel, highlight the **First Responder** label and right-click the mouse, or from the **File** menu, select **Add to First Responder**.



The **Add Configuration** dialog box opens displaying the **Parent Configuration** field already populated with the parent configuration. The **New Configuration** field is blank.


Add Configuration

Parent Configuration: First Responder

New Configuration:

2. For our First Responder example, in the **New Configuration** field, enter the title of the configuration to be associated with First Responder.
3. Click **Add New Configuration**.
   The new configuration label will now appear under the First Responder label.

Repeat this process for as many configurations as required to support a department's personnel or equipment to be equipped with an RSN. Note that this process should be completed for the entire list of configurations at this time. Once this is completed, RSNs can then be associated with each of the configurations defined in the tree. See Associating_RSNs_with_Configurations.

Canceling an Entry

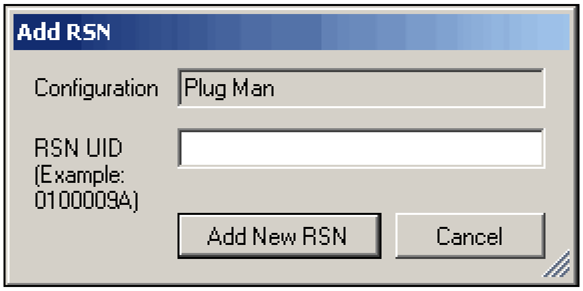
At any time during the data entry process, in the Add Configuration dialog box, should you decide the data is incorrect or not needed, click Cancel to close the dialog box and it will discontinue the "add new configuration" process.

8.2.8 Associating RSNs with Configurations

Associating an RSN to a configuration follows the same process as for creating the configuration.

To associate an RSN with a configuration, do the following:

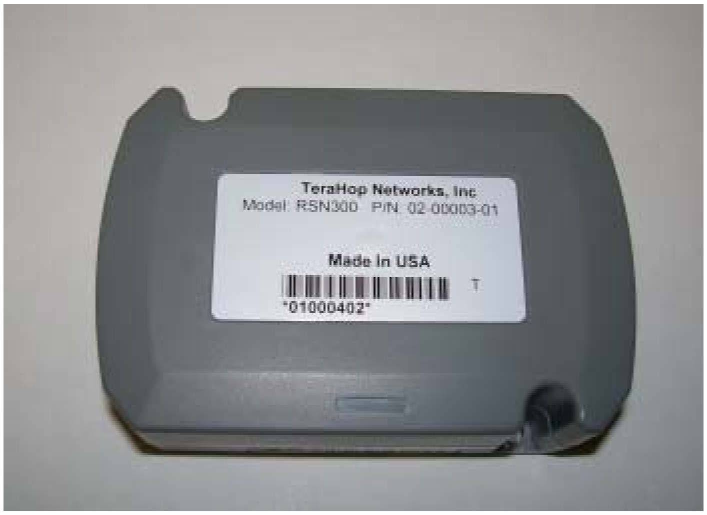
1. Highlight the configuration which an RSN is to be associated with.
2. Either right-click the mouse, or from the **File** menu select **Associate RSN to <name of Configuration>**.
   The **Add RSN** dialog box opens displaying the empty **RSN UID** field.


Add RSN

Configuration: Plug Man

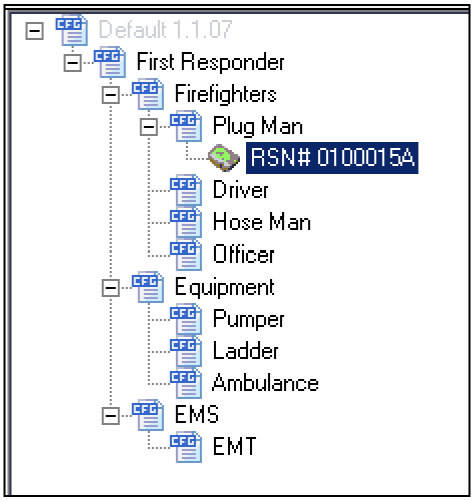
RSN UID (Example: 0100009A):

The RSN Unit ID (UID) can be found on the RSN itself or from a list provided with the equipment shipment. The UID is the number only, not the asterisks.



3. In the **RSN UID** field, enter the RSN UID.
   Enter the numbers only. Do not enter the asterisks.

4. Click **Add New RSN**.
   The RSN UID will now appear under the configuration with which it is associated in the configuration tree.

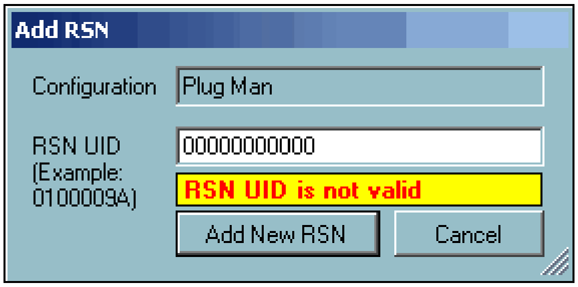


- Default 1.1.07
  - First Responder
    - Firefighters
      - Plug Man
        - RSN# 0100015A
      - Driver
      - Hose Man
      - Officer
    - Equipment
      - Pumper
      - Ladder
      - Ambulance
    - EMS
      - EMT

5. Continue this process for each of the RSNs that will be assigned.

Note that an RSN association can be made at any level on the configuration tree, even the default. An association at the default level is not recommended.

Note: If you enter an incorrect value in the RSN UID field, the following error message appears indicating the RSN UID is invalid and you should re-enter this value.

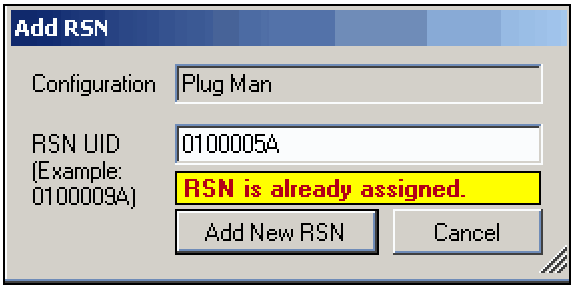


Configuration: Plug Man

RSN UID (Example: 0100009A): 00000000000

RSN UID is not valid

Each RSN UID is unique. If you enter a duplicate RSN UID, the following error message appears:



Configuration: Plug Man

RSN UID (Example: 0100009A): 0100005A

RSN is already assigned.

Note: At any time during the data entry process, should you decide the data is incorrect or not needed, click **Cancel** to close the dialog box and it will discontinue the RSN association process.

How to Remove an RSN From the Configuration tree

In the event an RSN needs to be removed from the left-hand configuration tree, you can delete it.

To remove an RSN from the left-hand configuration tree, do the following:

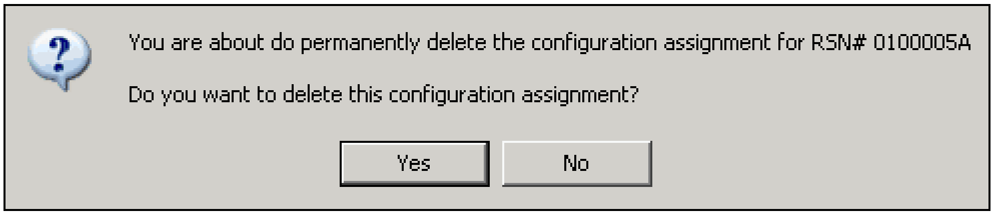
1. Highlight the RSN that needs to be removed.
2. Do one of the following.

   a. Right-click and select **Remove RSN # xxxxxxxxx**.

   Or,

   b. From the **File** menu, select **Remove RSN**.

   The *Remove Configuration Assignment* message appears asking you to confirm the removal of the RSN.



You are about do permanently delete the configuration assignment for RSN# 0100005A

Do you want to delete this configuration assignment?

3. To confirm the removal, click **Yes**. To cancel the removal, click **No**.

8.2.9 Modifying an RSN Configuration

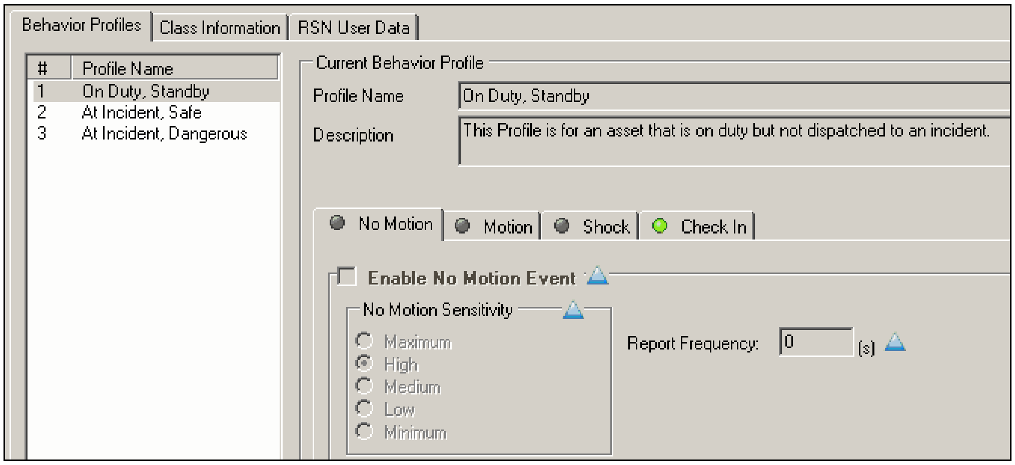
To modify a configuration, you should have previously created the configuration tree of the planned configurations. If this step has not been completed, refer to Creating a Left-Hand Configuration Tree, and complete this step before proceeding with this section.

To begin modifying a configuration, do the following:

1. Highlight the configuration in the configuration tree.

   Important!
   Keep in mind that this selection will define all of the parameters of those configurations defined under this selection.

   For example, in the illustration below, selecting Firefighters will set the defaults for all items listed under Firefighters; including Plug Man, Hose Man, etc. If the configuration were selected at the Plug Man level, only those under Plug Man would be subjected to the Plug Man configuration defaults - in this case, RSN 0100001A.
   Please note that these default profile names (On Duty, Standby, At Incident, Safe, or At Incident, Dangerous) in the top level may not be changed on any RSN configuration.



#	Profile Name
1	On Duty, Standby
2	At Incident, Safe
3	At Incident, Dangerous

Current Behavior Profile

Profile Name: On Duty, Standby

Description: This Profile is for an asset that is on duty but not dispatched to an incident.

□ Enable No Motion Event

No Motion Sensitivity
○ Maximum
● High
○ Medium
○ Low
○ Minimum

Report Frequency: 0 [s]

Behavior Profiles

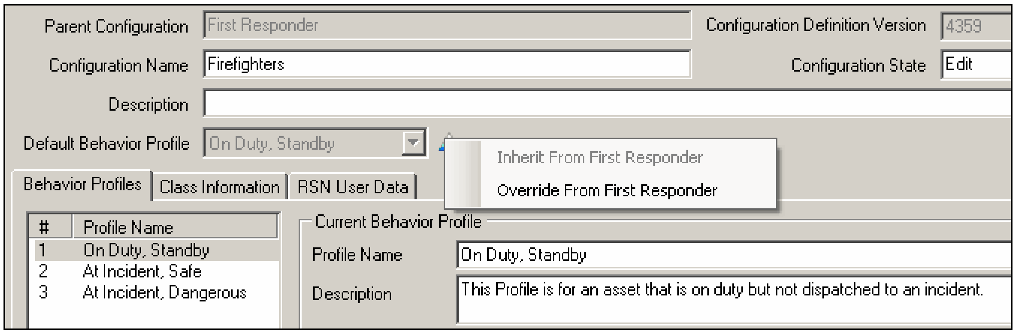
2. Look in the Middle section of the screen.
   This section is where the configuration parameters are defined.

3. Click the **Behavior Profiles** tab.
   Initially, three Behavior Profiles are supported (more will be supported in a future release). As shown in our First Responder Plug Man example, begin by selecting the first **Behavior Profile** with a default label of **On Duty, Standby** as shown above. Moving to the right of this selection, the parameter settings for this profile are displayed. These parameters have been inherited from the Firefighter configuration from the configuration tree and each of these parameters can be edited for the specific requirements of the Plug Man.

   Editing Behavior Profiles

   The items that are inherited can be identified by the blue vertical triangle next to the parameter description or selection. Where these values have been inherited from can be determined by hovering over the blue triangle (i.e., which configuration in the configuration tree).
   Note: Fields that cannot be edited are gray, and their adjacent triangles are also gray.

4. To edit an inherited parameter, right click on the upward-facing blue triangle adjacent to the label.
   In our First Responder example, the **Override From First Responder** pop-up opens.

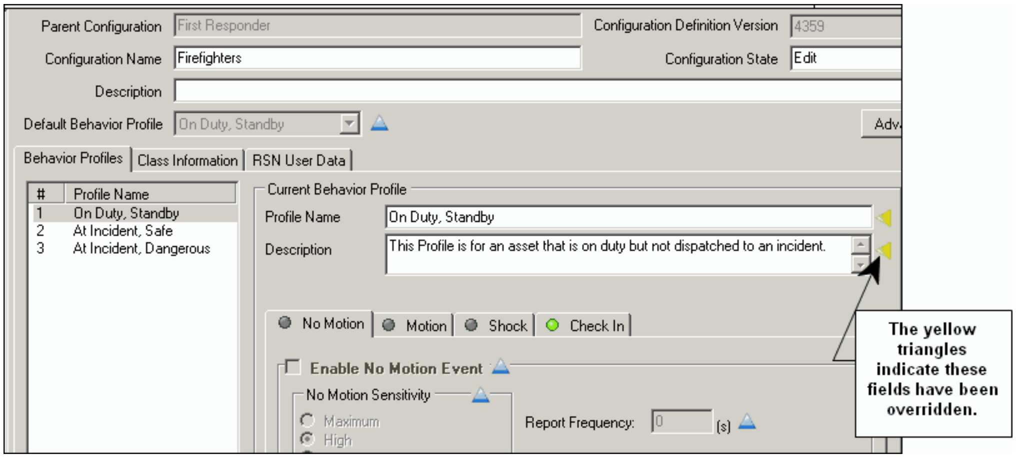


Parent Configuration: First Responder
Configuration Definition Version: 4359
Configuration Name: Firefighters
Configuration State: Edit
Description:
Default Behavior Profile: On Duty, Standby

#	Profile Name
1	On Duty, Standby
2	At Incident, Safe
3	At Incident, Dangerous

Current Behavior Profile
Profile Name: On Duty, Standby
Description: This Profile is for an asset that is on duty but not dispatched to an incident.

5. Select **Override from First Responder** (the configuration name).
   The field is no longer gray and becomes available for editing, as illustrated below for the **Profile Name** and **Description** fields. Notice that the blue upward-facing triangle is now a left-facing yellow triangle.



Parent Configuration: First Responder
Configuration Definition Version: 4359
Configuration Name: Firefighters
Configuration State: Edit
Description:
Default Behavior Profile: On Duty, Standby

#	Profile Name
1	On Duty, Standby
2	At Incident, Safe
3	At Incident, Dangerous

Current Behavior Profile
Profile Name: On Duty, Standby
Description: This Profile is for an asset that is on duty but not dispatched to an incident.

□ Enable No Motion Event
No Motion Sensitivity
○ Maximum
● High
Report Frequency: 0 [s]

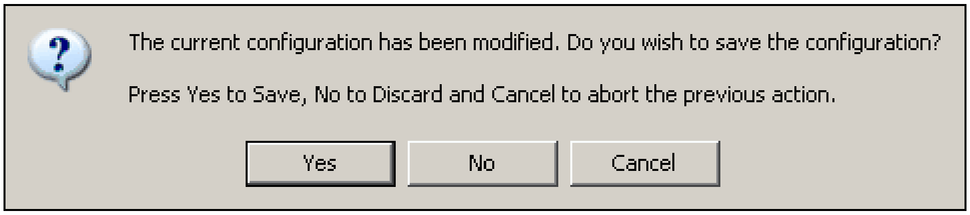
The yellow triangles indicate these fields have been overridden.

6. Make the desired edits for this field.
   Similar edits can be completed as necessary for the fields in other remaining configurations.

Saving Changes

7. When you have finished making changes, click the **Save Configuration** button located at the bottom of the right-hand panel.
   At any time should you need to return to the original default parameters, before you save the changes, click the **Undo Changes** button at the bottom of the right-hand panel.

   The application also will not allow you to navigate away from a page that has been edited without being saved. Should you edit a parameter setting and then navigate away prior to saving the new configuration, a pop-up box appears asking if you would like to save the recent changes.



The current configuration has been modified. Do you wish to save the configuration?

Press Yes to Save, No to Discard and Cancel to abort the previous action.

8. If you see the message shown above, do one of the following:
   a. To save the changes, click **Yes.**
   b. To disregard the changes, click **No**.
   c. To abort the previous action, click **Cancel**.

   The Behavior Profile parameters for each Profile can now be defined. That is, each of the three Behavior Profiles can be configured independently. As with the Profile Name and Description, the application is provided with default values for each of the available Behavior Profile parameters and each can be changed as previously described.

9. Continue to Configuring RSN Sensors.

8.2.10 Configuring RSN Sensors

Each RSN is equipped with internal sensors that provide specific capabilities to assure proper operation of the RSN while ensuring the safety of the person or equipment associated with the RSN. These sensor settings are defined within the RCT under the Behavior Profiles tab. To accomplish the sensor configuration, the application has three tabs that are used to define each sensor functions along with a tab for defining the RSN check-in time.

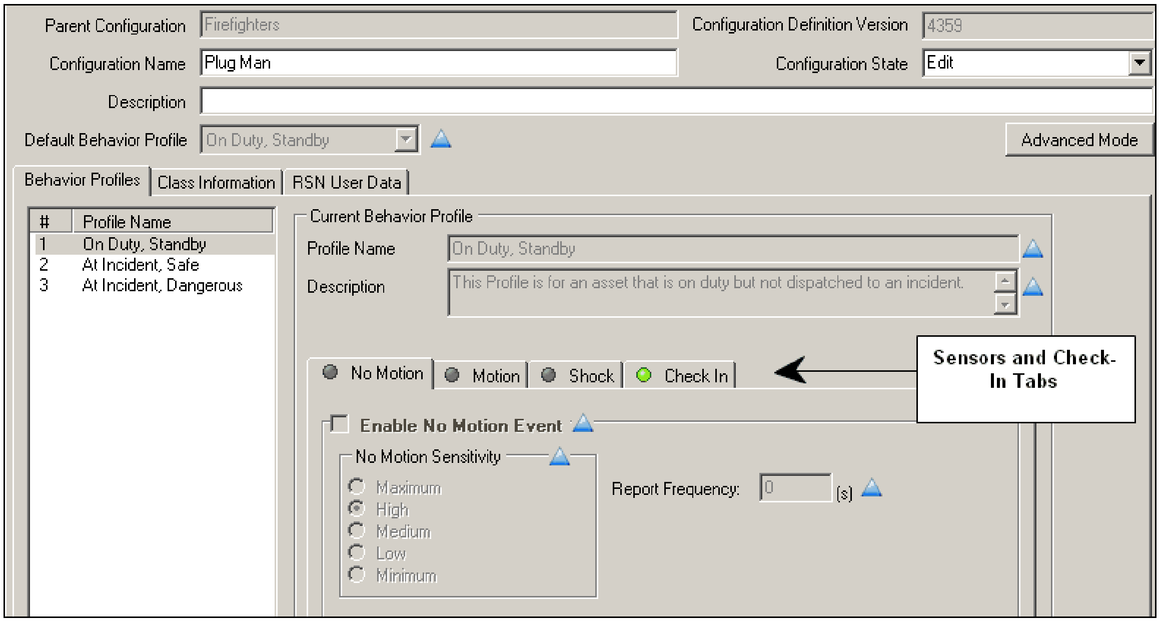
For the initial release, the sensors supported in the RSN are mutually exclusive for a given profile. That is, an RSN's behavior profile cannot have both a Motion and Shock sensor enabled within a single configuration. The RCT is designed to prevent you from allowing this configuration to take place.

In addition to the **Check-in** tab, the supported RSN sensors and their associated tabs are:

- No-Motion
- Motion
- Shock

8.2.10.1 No-Motion

The No-Motion sensor is used to determine when an asset carrying an RSN is expected to be in motion for a defined duration, but is not. The enabling of this sensor, its sensitivity, along with the no-motion duration, is configurable under the **No Motion** tab. The **Report Frequency** is a setting that defines the amount of time (in seconds) that must pass before another event alarm is sent to the user application. It is recommended that this setting remain at zero, which will issue an alarm for each event occurrence.



Parent Configuration: Firefighters

Configuration Definition Version: 4359

Configuration Name: Plug Man

Configuration State: Edit

Description:

Default Behavior Profile: On Duty, Standby

#	Profile Name
1	On Duty, Standby
2	At Incident, Safe
3	At Incident, Dangerous

Current Behavior Profile

Profile Name: On Duty, Standby

Description: This Profile is for an asset that is on duty but not dispatched to an incident.

□ Enable No Motion Event

No Motion Sensitivity

○ Maximum
● High
○ Medium
○ Low
○ Minimum

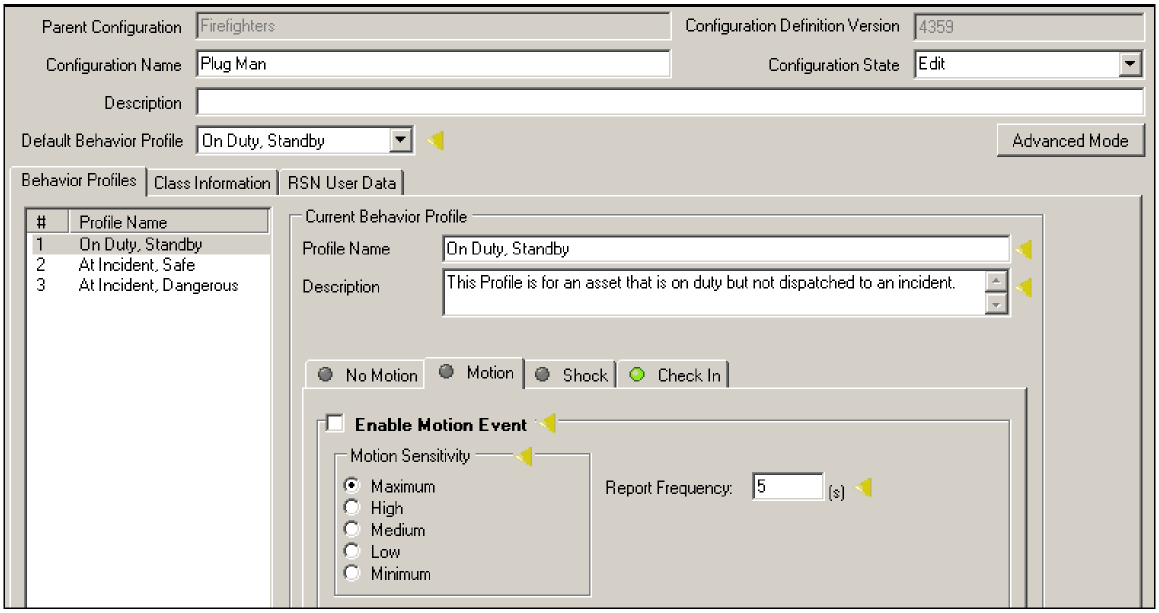
Report Frequency: 0 (s)

To configure this functionality, do the following:

1. Click the **No Motion** tab.
2. To enable **No-Motion** under this **Behavior Profile**, override and click the **Enable No Motion Event** checkbox.
3. In the same manner, override the **No Motion Sensitivity** radio button selection.
4. Click to select the desired **Sensitivity level** radio button.
   Note: it is recommended that the default sensitivity be selected until ample field experience is obtained to justify a more or less sensitivity selection.

Motion

The Motion sensor is used to determine when an asset carrying an RSN is in motion for a defined duration when it is not expected to be. The enabling of this sensor, reporting, its sensitivity, along with the motion duration, are configurable under the **Motion** tab. The **Report Frequency** is a setting that defines the amount of time (in seconds) that must pass before a repeat event alarm is sent to the user application. It is recommended that this setting remain at zero, which will issue an alarm for each event occurrence.



Parent Configuration: Firefighters
Configuration Definition Version: 4359
Configuration Name: Plug Man
Configuration State: Edit
Description:
Default Behavior Profile: On Duty, Standby

#	Profile Name
1	On Duty, Standby
2	At Incident, Safe
3	At Incident, Dangerous

Current Behavior Profile
Profile Name: On Duty, Standby
Description: This Profile is for an asset that is on duty but not dispatched to an incident.

□ Enable Motion Event

Motion Sensitivity
● Maximum
○ High
○ Medium
○ Low
○ Minimum

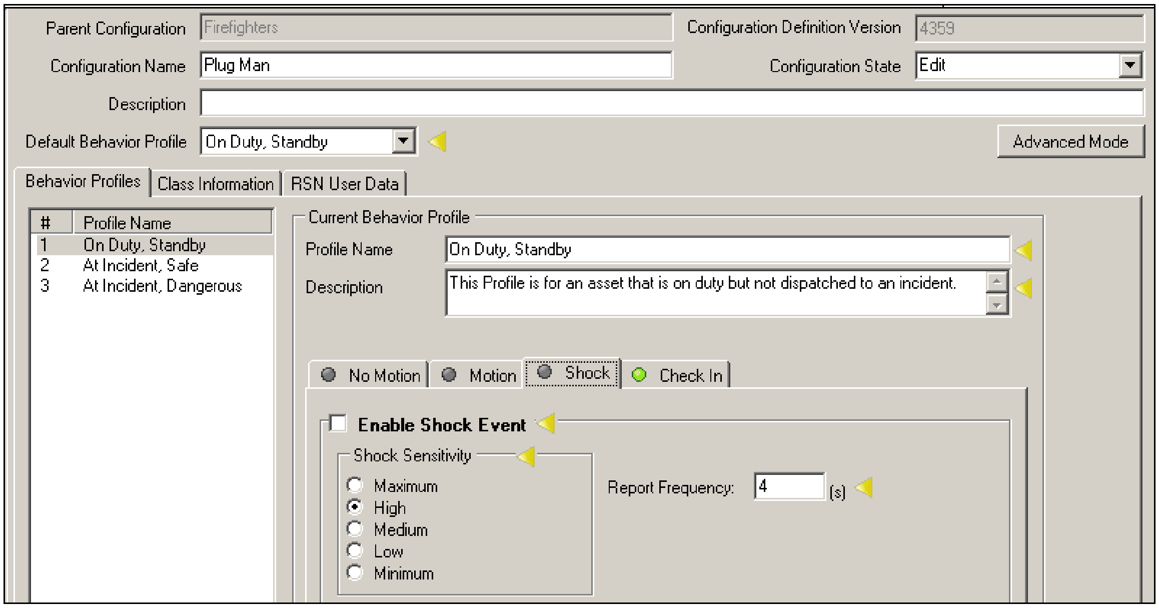
Report Frequency: 5 (s)

To configure the Motion sensor, do the following:

1. Click the **Motion** tab.
2. To enable Motion under this Behavior Profile, override and select the **Enable Motion Event** check box.
3. In the same manner, override the **Motion Sensitivity** radio buttons selections.
4. Click to select the desired **Sensitivity level** radio button.
   Note: it is recommended that the default sensitivity be selected until ample field experience is obtained to justify a different sensitivity selection.

Shock

The Shock sensor is used to determine when an asset has been struck with a predetermined force. The enabling of this sensor, its sensitivity, along with the number of shock events to issue an alarm is configurable under the **Shock** tab. The **Report Frequency** is a setting that defines the amount of time (in seconds) that must pass before another event alarm is sent to the user application. It is recommended that this setting remain at four (4), which will issue an alarm no more often than once every four (4) seconds.



Parent Configuration: Firefighters
Configuration Definition Version: 4359
Configuration Name: Plug Man
Configuration State: Edit
Description:
Default Behavior Profile: On Duty, Standby

#	Profile Name
1	On Duty, Standby
2	At Incident, Safe
3	At Incident, Dangerous

Current Behavior Profile
Profile Name: On Duty, Standby
Description: This Profile is for an asset that is on duty but not dispatched to an incident.

☐ Enable Shock Event
Shock Sensitivity
○ Maximum
● High
○ Medium
○ Low
○ Minimum
Report Frequency: 4 (s)

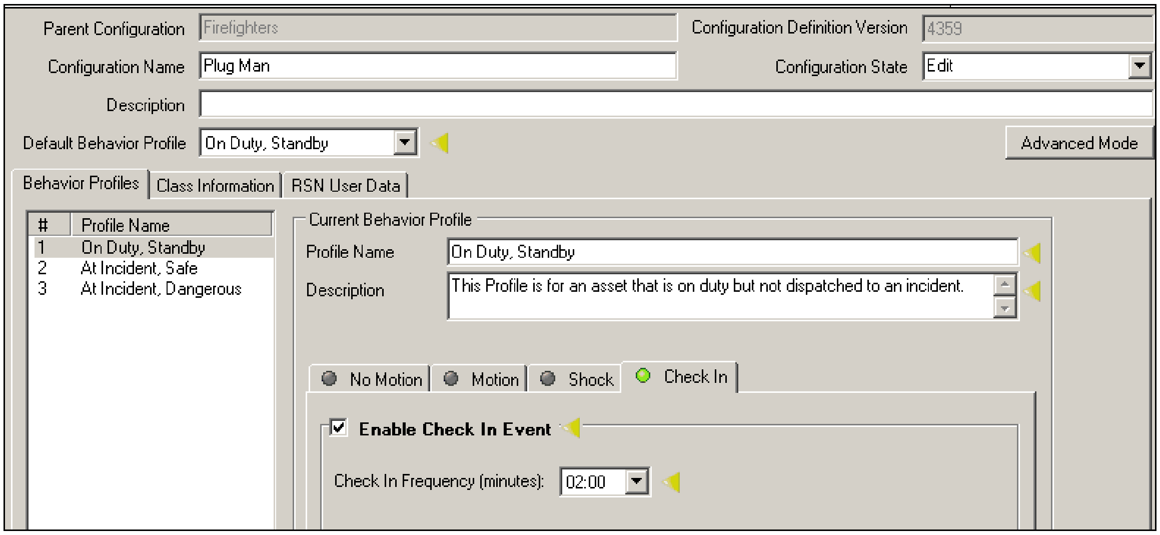
To configure the Shock sensor, do the following:

1. Click the **Shock** tab.
2. To enable Shock under this Behavior Profile, override the **Enable Shock Event** label and select the **Enable Shock Event** check box.
3. In the same manner, override the **Shock Sensitivity** radio buttons selection.
4. Click to select the desired **Sensitivity** level radio button.

Note: it is recommended that the default sensitivity be selected until ample field experience is obtained to justify a more or less sensitivity selection.

Check-in

The Check-in is used to specify the frequency at which the RSN checks in with the TeraHop network to confirm its presence. Depending on the behavior profile, a more frequent check-in rate may be desired. For example, a First Responder asset assigned to a dangerous task would want a faster check-in rate than one in Re-hab.



Parent Configuration: Firefighters

Configuration Definition Version: 4359

Configuration Name: Plug Man

Configuration State: Edit

Description:

Default Behavior Profile: On Duty, Standby

#	Profile Name
1	On Duty, Standby
2	At Incident, Safe
3	At Incident, Dangerous

Current Behavior Profile

Profile Name: On Duty, Standby

Description: This Profile is for an asset that is on duty but not dispatched to an incident.

☑ Enable Check In Event

Check In Frequency (minutes): 02:00

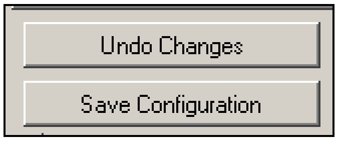
To configure the Check-in parameter, do the following:

1. Click the **Check-in** tab.
   The **Check-in** selection should always be enabled, and the only parameter that should be configured is the Check-in Frequency.
2. To change the Check-in, override the **Check-in Frequency** drop-down box.
3. In the **Check-in Frequency** field, click the drop-down arrow and select the desired check-in frequency from the drop-down list of values.

8.2.11 Saving the Configurations

It is recommended that you save the configuration changes after each tab has been edited. However, saving more often is a good policy. Also note that should at any time it be required to return to the original default parameters, this can be achieved, prior to the changes being saved, by selecting the Undo Changes button at the bottom of the middle section.

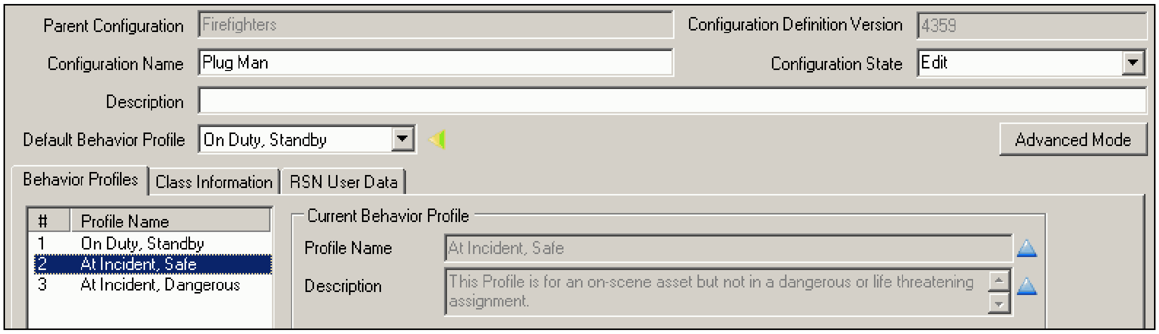
To save a configuration, click the **Save Configuration** button located at the bottom of the right-hand panel.



8.2.12 Default Behavior Profile

Once all of the Behavior Profile settings have been configured, the Default Behavior Profile for each of the left-hand configurations can be selected. The Default Behavior Profile is the Behavior Profile the RSN associated with a configuration will operate under until changed by a user application. This field is located towards the top of the Middle section above the Configuration Parameter tabs.

In the example we have been using, the Default Behavior Profile for the Plug Man is On Duty, Standby. This is the Profile he will remain under until a user application changes his assignment to one that uses At Incident, Safe or At Incident, Dangerous.



Parent Configuration: Firefighters

Configuration Definition Version: 4359

Configuration Name: Plug Man

Configuration State: Edit

Description:

Default Behavior Profile: On Duty, Standby

#	Profile Name
1	On Duty, Standby
2	At Incident, Safe
3	At Incident, Dangerous

Current Behavior Profile

Profile Name: At Incident, Safe

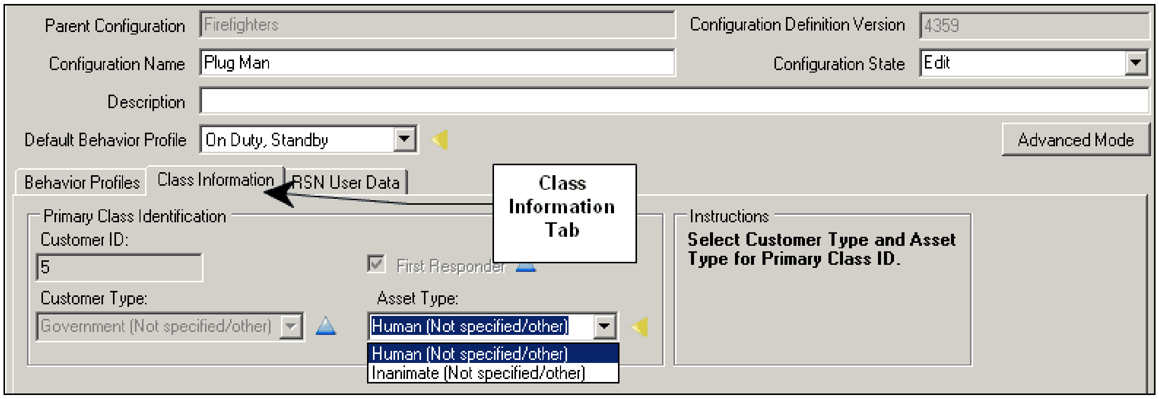
Description: This Profile is for an on-scene asset but not in a dangerous or life threatening assignment.

To change the default profile, do the following:

1. Override the default for the **Default Behavior Profile** field.
2. In the **Default Behavior Profile** field, click the drop-down arrow.
   The list of available behavior profiles for this configuration appears.
3. Select the desired Default Profile from the available drop-down list.
4. Click the **Save Configuration** button at the bottom of the Middle section.

8.2.13 Class Information

The **Class Information** tab is used to define the TeraHop network with which the configured RSNs can communicate, whether it is a TeraHop network generated by the organization configuring the RSNs or one that is joined in a merge or mutual aide scenario. As the defaults are already set for the First Responder market, no changes to the parameters defined under this tab should be required unless the RSN Asset Type is to be associated with a piece of equipment rather than an individual.



Parent Configuration: Firefighters
Configuration Definition Version: 4359
Configuration Name: Plug Man
Configuration State: Edit
Description:
Default Behavior Profile: On Duty, Standby

Primary Class Identification
Customer ID: 5
☑ First Responder
Customer Type: Government (Not specified/other)
Asset Type: Human (Not specified/other)

Instructions
Select Customer Type and Asset Type for Primary Class ID.

To edit the Asset Type parameter, do the following:

1. Click the **Class Information** tab.

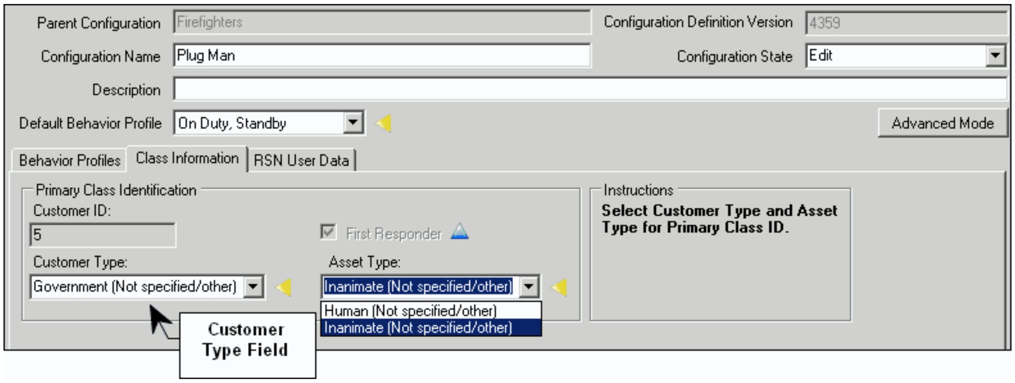
2. Override the default for the **Asset Type** field.

3. In the **Asset Type** field, click the drop-down arrow and select **Inanimate**.

8.2.14 Customer Type Default

As the default configuration is for First Responders, the Customer Type default is set for Government. However, should the configuration be for a commercial entity, do the following:

1. Click the **Class Information** tab, if necessary.
2. Override the default for the **Customer Type** field.
3. In the **Customer Type** field, click the drop-down arrow and select the configuration option.
   For the First Responder market, Government should always be selected.
4. Click the **Save Configuration** button at the bottom of the Middle section.
   The Customer ID is a fixed number assigned by TeraHop Networks and cannot be edited from this screen.



Parent Configuration: Firefighters
Configuration Definition Version: 4359
Configuration Name: Plug Man
Configuration State: Edit
Description:
Default Behavior Profile: On Duty, Standby

Primary Class Identification
Customer ID: 5
☑ First Responder
Customer Type: Government (Not specified/other)
Asset Type: Inanimate (Not specified/other)

Instructions
Select Customer Type and Asset Type for Primary Class ID.

8.2.15 Additional Assets

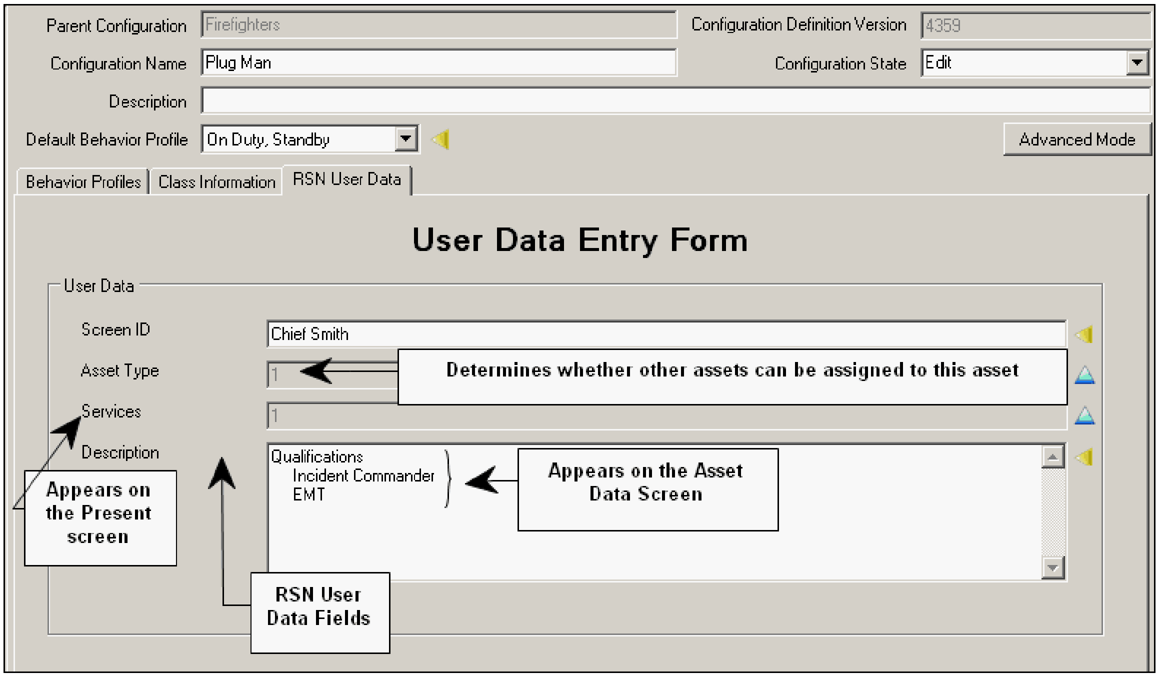
For each of the configurations in the left-hand panel of the application, complete the above-defined process. As previously discussed, the layout of the left-hand structure and the use of the inheritance feature can greatly reduce the overall number of unique configurations required to support the configurations for each RSN.

8.2.16 RSN User Data

The remaining Behavior Profile tab, **RSN User Data**, is for configuring parameters at the RSN level rather than at the asset type from the left hand tree section of the Tool. In order to configure a specific RSN with the remaining parameter, highlight the RSN that is to be configured.

In our on-going example, Plug Man’s RSN Number 0100001A has been selected. The parameters for the tab are described in the next section.

8.2.16.1 User Data Entry Form



Parent Configuration: Firefighters
Configuration Definition Version: 4359
Configuration Name: Plug Man
Configuration State: Edit
Description:
Default Behavior Profile: On Duty, Standby

User Data Entry Form

User Data

Screen ID: Chief Smith
Asset Type: 1
Services: 1
Description: Qualifications
Incident Commander
EMT

Determines whether other assets can be assigned to this asset

Appears on the Asset Data Screen

Appears on the Present screen

RSN User Data Fields

The RCT provides the user with access to a block of memory within the RSN to enter specific data. The data that is placed in this area is for information only and is what is displayed on the user application when an asset is accessed.

To edit each of these fields, right click on the blue triangle next to each data field. Select the Override option from the pop-up window. The data entry field is no longer gray and can be edited. Enter the desired information into the data field.

The **Screen ID** is typically the name of the asset the RSN is assigned to, such as Chief Smith or Engine 42. The way the data is entered and formatted into this field is how it will be displayed within the user application.

The **Description** is a free-form data entry field where any applicable information about the asset can be added. This may include specifications about a piece of equipment or specific qualifications of an individual. The Tool provides this capability for download at the RSN configuration time. It is recommended that the Screen ID be the first entry into this data field.

The RSN does not look at, use, or write into this area of memory, except as directed during the configuration and through special application level read/write access to this section of memory.

The **Service** is the department or organization with which the RSN is associated. The default service is set for 1; Fire, rescue. The following services are applicable entries:

Reference Number	Description	Application Screen Label
1	Fire, rescue	FR
2	Police, sheriff, DA	LE
3	EMS, ambulance, medical	EM
4	Utilities and roads	PW
5	Public Health	PH
6	Military	ML
7	Visitor	V
8	Administration and Other	A/O

Asset Type is a numerical reference that the IMS uses to identify the kind of asset to which an RSN is attached. The IMS PDA displays data differently depending on whether an asset is a person or unit/vehicle, etc. The choices for Asset Type that are available in the RCT are:

Ref. #	Corresponding Asset Type
1	Individual person
2	Commander
3	Unit/Vehicle*
4	Equipment (not associated with a Unit)
5	K9

*On the PDA, other assets (except a unit) can be assigned to this asset type.

8.2.17 How to Wake Up or Troubleshoot an RSN

TeraHop Remote Sensor Nodes (RSNs) are shipped from the factory to the Channel Partner. They are shipped in a deep sleep, and you need to 'wake' them up before you can configure them for an end customer.

To wake up an RSN, you will use the RSN Configuration Tool (RCT) Cradle. The RCT Cradle is a device with a 16-pin connector and LEDs to indicate the status of the RSN. The RCT Cradle includes an RSN that has been tested and is known to be good.

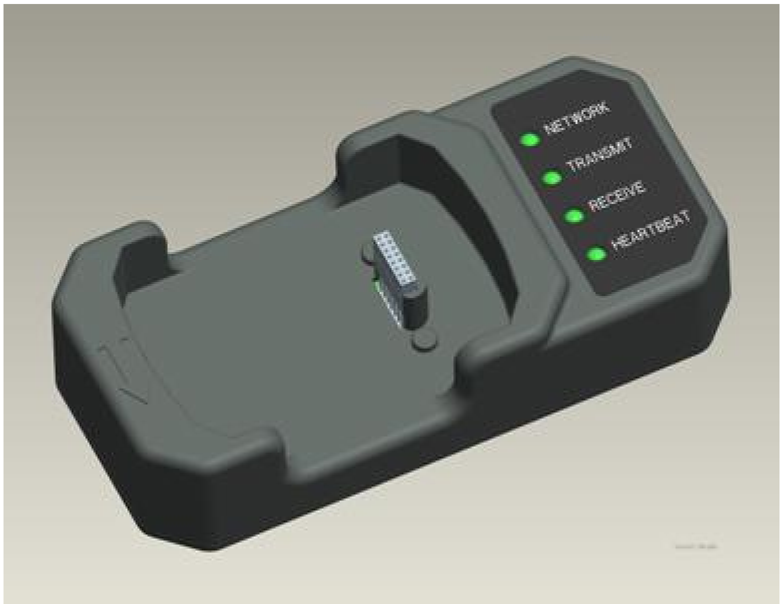
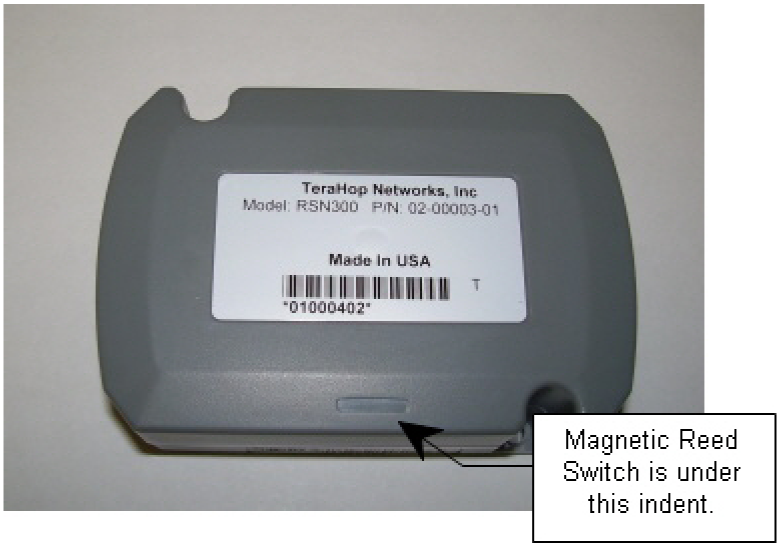


Figure 15: RCT Cradle

The RSN has a shallow indent on the top of it. The Magnetic Reed Switch is under this indent.



Magnetic Reed Switch is under this indent.

Figure 16: Magnetic Reed Switch Indent on RSN

The RSN has a plug on the back that is removed during the wake-up procedure.

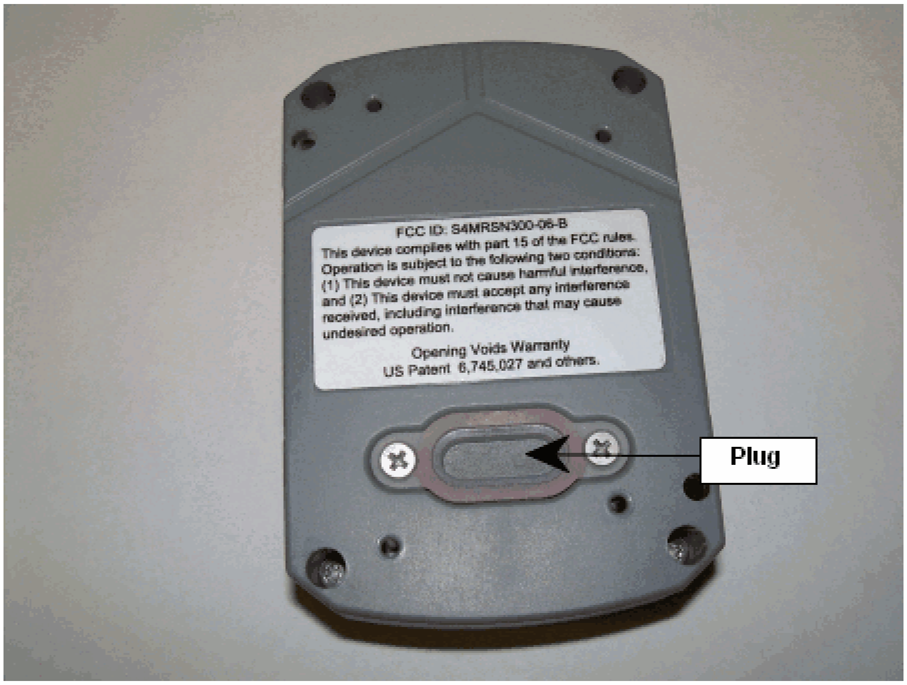

FCC ID: S4MRSN300-06-B
This device complies with part 15 of the FCC rules.
Operation is subject to the following two conditions:
(1) This device must not cause harmful interference,
and (2) This device must accept any interference
received, including interference that may cause
undesired operation.
Opening Voids Warranty
US Patent 6,745,027 and others.
Plug

Figure 17: Plug on RSN

The RCT Cradle has an indicator on one end (see the illustration below). The other end of the RCT Cradle has a plug. This plug is used to attach the RCT Cradle to the laptop computer with the provided USB cable when you download RSN configuration data you have set up on the laptop computer using the RSN Configuration Tool or when you want to troubleshoot an RSN.

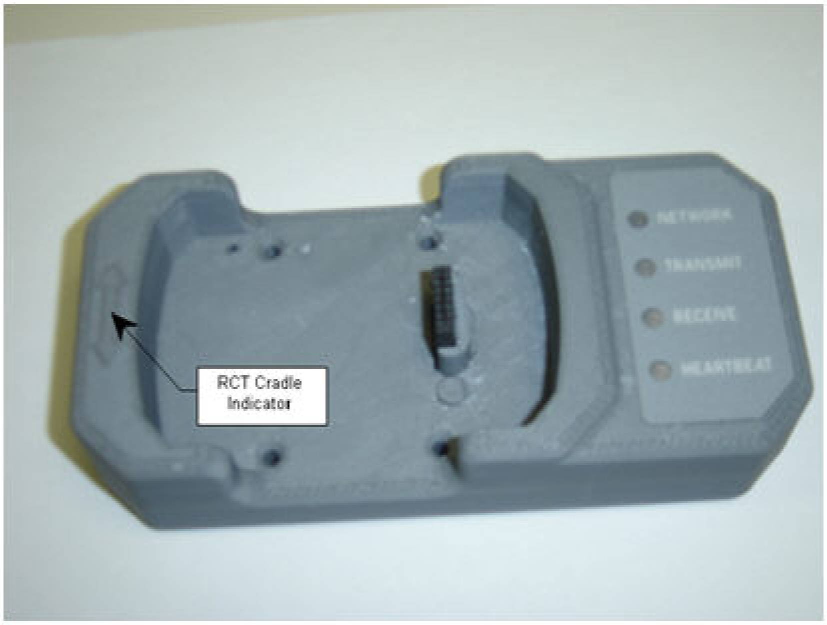


Figure 18: Indicator on RCT Cradle

To wake up an RSN, do the following:

1. Remove the plug from the underside of the RSN.
2. Swipe the RSN indent next to the cradle indicator to activate the Magnetic Reed Switch. The cradle indicator looks like a two-headed arrow embossed on the top of the cradle.
3. Place the RSN in the RCT Cradle so that the hole in the RSN fits snugly over the 16-pin connector on the cradle.

   You should see the Heartbeat LED light (#4 illustrated below).

   You should then see the NETWORK, TRANSMIT, and RECEIVE LEDs light in that order (numbers 1, 2, and 3 in the illustration below). When the LEDs light, you know that the RSN is good.

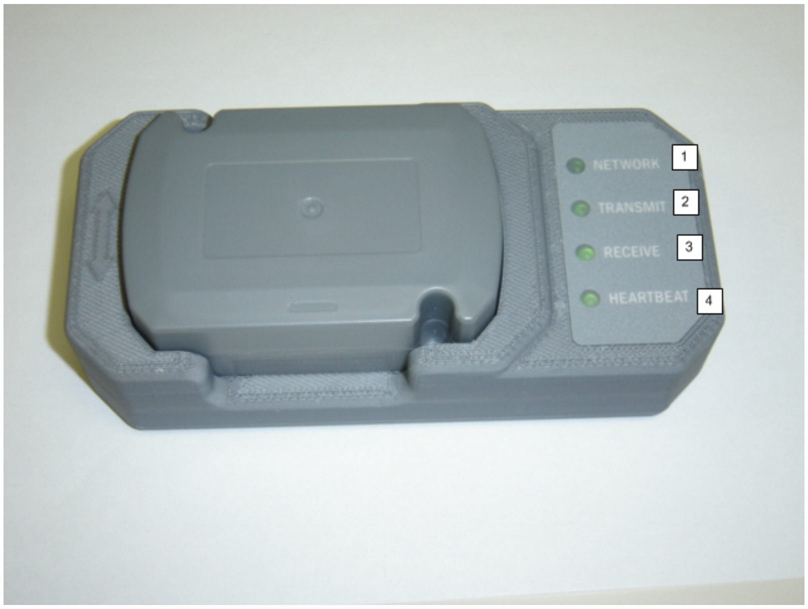


Figure 19: RCT Cradle LEDs

8.2.17.1 Troubleshooting the RSN

Using the same technique above, place the RSN you want to test in the RCT Cradle.

If you see the heartbeat LED is lit, then you know that the RSNs is working. If the RSN is still not working (receiving or transmitting), then the trouble is with another component in the IMS.

Using the illustration above, you can see the status of the LEDs on the RCT Cradle. Using the RSN Troubleshooting Solutions table below, if an LED is not lit, look at the possible causes in the Not Illuminated column. For a possible solution to why the LED is not illuminated, look in the Description and Resolution columns.

Table 6: RSN Troubleshooting Solutions

LED Indicator	Description	Resolution
1. NETWORK	If illuminated, the RSN has joined a network.	
2. TRANSMIT	If illuminated, the RSN wake-up radio is transmitting.	
3. RECEIVE	If illuminated, the RSN wake-up radio is receiving.	
4. HEARTBEAT	If flashing at a 1Hz rate, the RSN radio is enabled.	
No LEDs illuminated	RSN is not enabled.	Enable the RSN.
No LEDs illuminated	RSN is in deep sleep.	Awaken the RSN.
No LEDs illuminated	RSN is in shutdown.	Reset the RSN (press the black power switch in the RSN plug cavity).
No LEDs illuminated	Battery is dead.	Return to TeraHop Networks for battery replacement.
4. Only HEARTBEAT is illuminated.	HEARTBEAT not receiving. RSN not hearing a Gateway beacon.	Ensure the RSN is in range of a Gateway, at least 300' without RF interference. Verify the paging channel is set properly to 78. To verify, in the RCV, select the Engineering level, and click Get RSN data. Look in the middle section of the

LED Indicator	Description	Resolution
		screen under RCR Parameters for Paging Channel. This should be 78. If it is not, return the RSN to TeraHop Networks.
NETWORK (1), then **HEARTBEAT (4)**, then **HEARTBEAT (1)** illuminate.	The RSN suddenly returns to the HEARTBEAT while trying to register on the network.	The registration has been rejected. Check the Class ID using the RCT.
Bounces from **HEARTBEAT (4)** to **NETWORK (1)** back and forth.	Never gets registered on the network.	RSN is still waiting for a response to the registration request.
All LEDs are flashing.	RSN is not responding. RSN is constantly resetting.	RSN failed to get an EEPROM signature. Reset the RSN by pressing the black power switch in the RSN plug cavity. If no change, return the RSN to TeraHop Networks.

8.2.18 Downloading an RSN Configuration

Once all of the configuration parameter settings have been completed, the configuration is now ready to be downloaded into an RSN. At the bottom of the left-hand panel configuration tree there is a Program RSN section.

To configure an RSN via a direct connect to the PC, you will need a THN RCT Cradle, a USB cable, and the RSN Configuration Tool (RCT).

8.2.18.1 Notes on Using the RCT Cradle

- Do not leave an RSN in the cradle for an extended period of time. After you have completed your RSN test or download, immediately remove the RSN from the cradle.
- While running the download application, never unplug the USB cable, whether or not an RSN is in the cradle. Always close the RCT application before unplugging the USB cable.
- Although the RSN will work with very little pressure in the cradle, it is recommended that you push the RSN to the bottom of the cradle so that it is completely seated.
- If you place an RSN in the cradle and there is no cradle light activity (blinking or solid) on the RSN, remove the RSN and swipe it near the cradle magnet. Then try it again. If the result is the same, depress the end of the black power switch inside the RSN plug cavity for 10 seconds. Then try it again in the cradle. If the result is the same, return the

RSN. This should only be attempted by someone qualified to perform this operation; i.e., someone who has been trained how to do it.

- If there is cradle light activity but no communication with the RSN, then restart the application used to communicate with the RSN. If the result is the same, return the RSN.

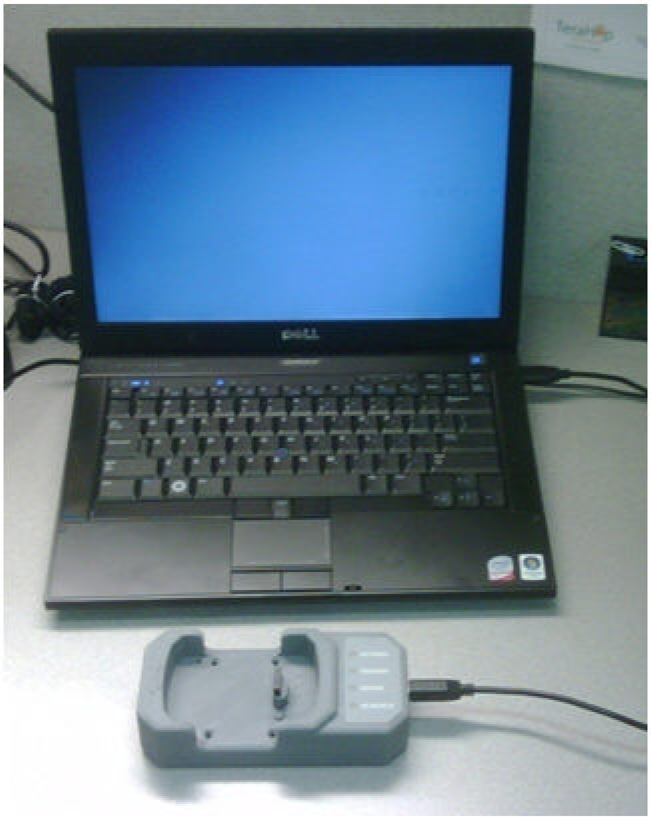
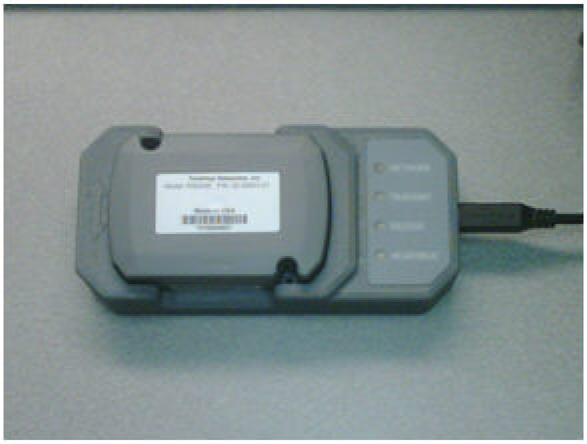


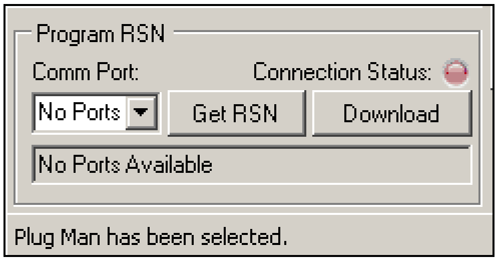
Figure 20: RCT Cradle Attached to ADMS Laptop Computer

To complete the RSN configuration, follow these steps:

1. Plug one end of the USB cable into the PC USB port and the other end into the RCT Cradle.
2. Connect the RSN to a RCT Cradle.



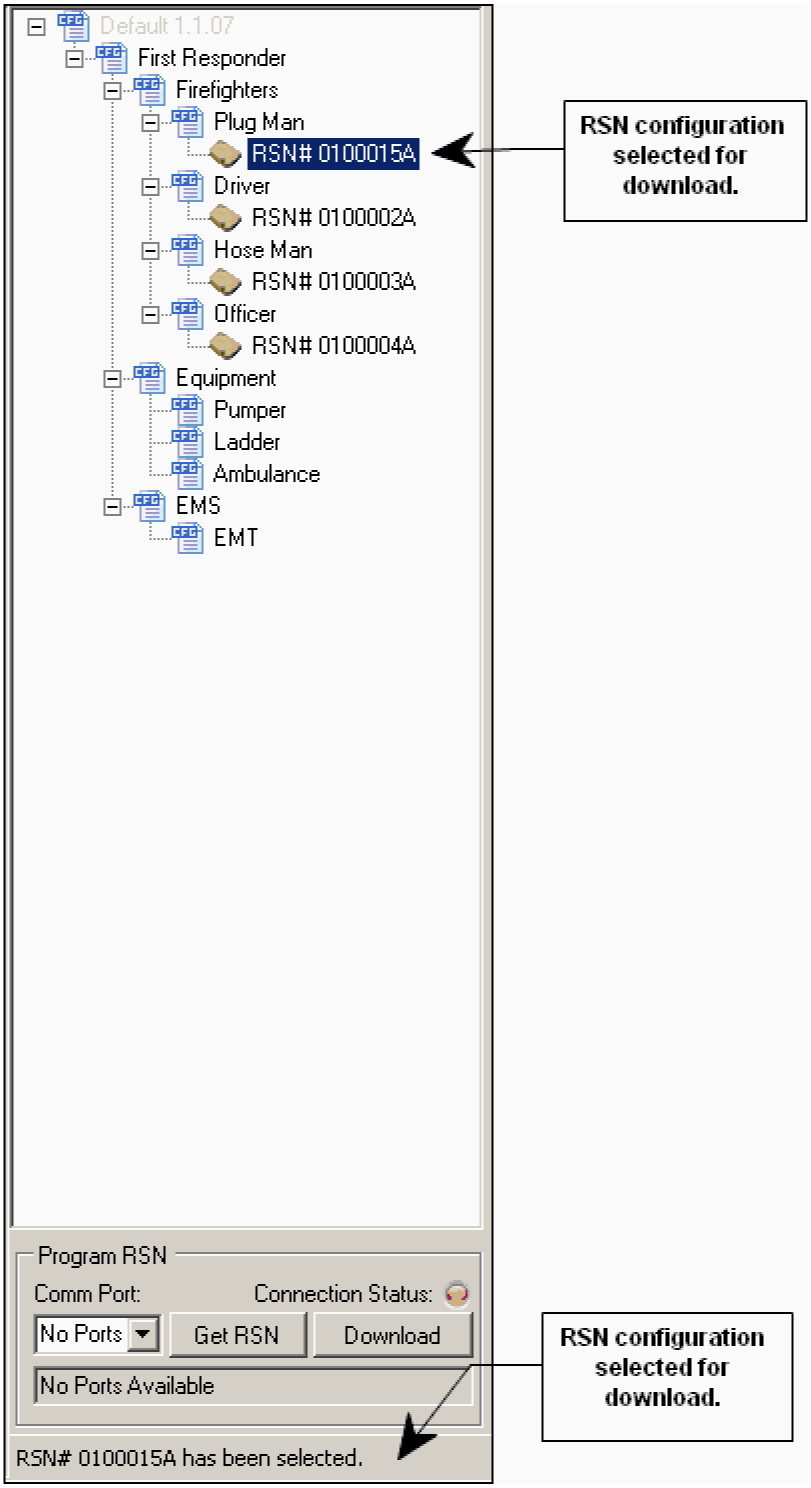
3. In the RCT on the laptop computer, in the lower left section of the screen, you will see the **Program RSN** section.



No Ports Available

Plug Man has been selected.

4. Under **Comm Port**, click the drop-down list and select the correct Comm Port for use with this device.
5. Click **Get RSN**.
   The RCT will attempt to connect to the RSN and read its Unit ID (UID).
   In a status box at the bottom of the Program RSN section, the application will report that it has found an RSN, if the RSN has the right software version, and if that RSN has been associated with a configuration in the tree above. The RSN configuration will be highlighted in the left-hand panel. Once these parameters have been verified the associated configurations will automatically be selected and the download button will be enabled.
6. Click the **Download** button.



No Ports Available

RSN# 0100015A has been selected.

RSN configuration selected for download.

RSN configuration selected for download.

The status bar will display status messages of the download progress. Upon completion, the status bar will turn green to indicate success or red to indicate failure.

7. Once a successful download has been completed, remove the RSN from the sled and repeat the process with another RSN.

When selected, the window displays the download status information as well as the history of the status messages.

Immediately after downloading the configuration, the RSN is reset automatically, causing it to restart with the new configuration settings. When the RSN restarts, the default behavior profile is selected.

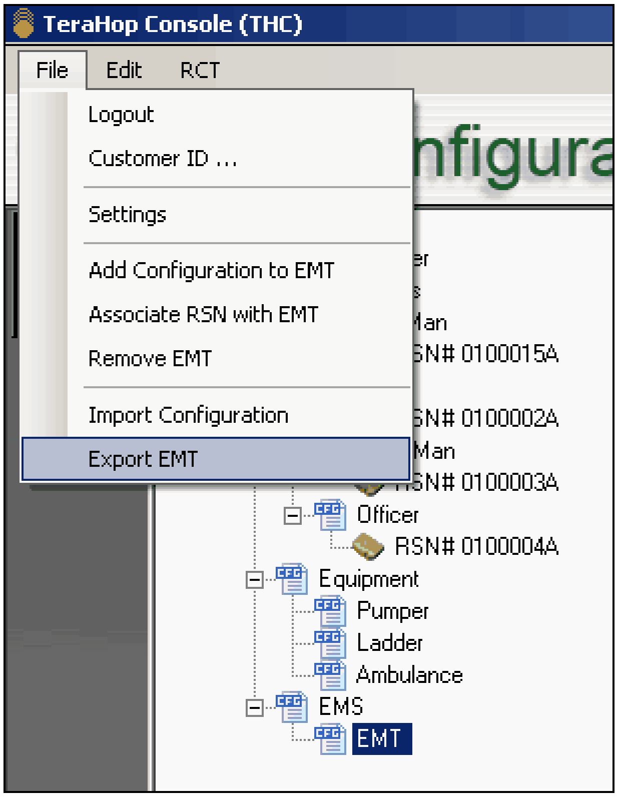
8.2.19 RSN Configuration Import / Export

8.2.19.1 Export

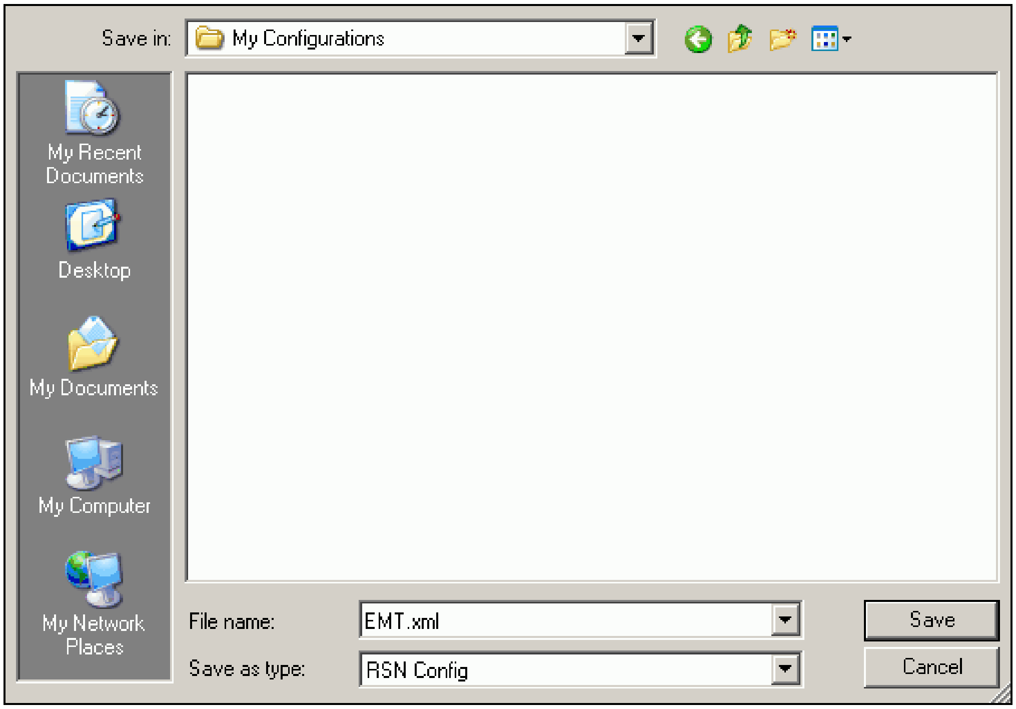
As each configuration is a separate entity, a configuration can be imported and exported between RCT users for sharing and re-use.

To export a configuration, do the following:

1. From the configuration tree, click to select the configuration.



2. From the **THC** menu, select **File** and then **Export <configuration>**.
   A standard MS Windows Save window titled **Save Configuration File** opens.



File name: EMT.xml

Save as type: RSN Config

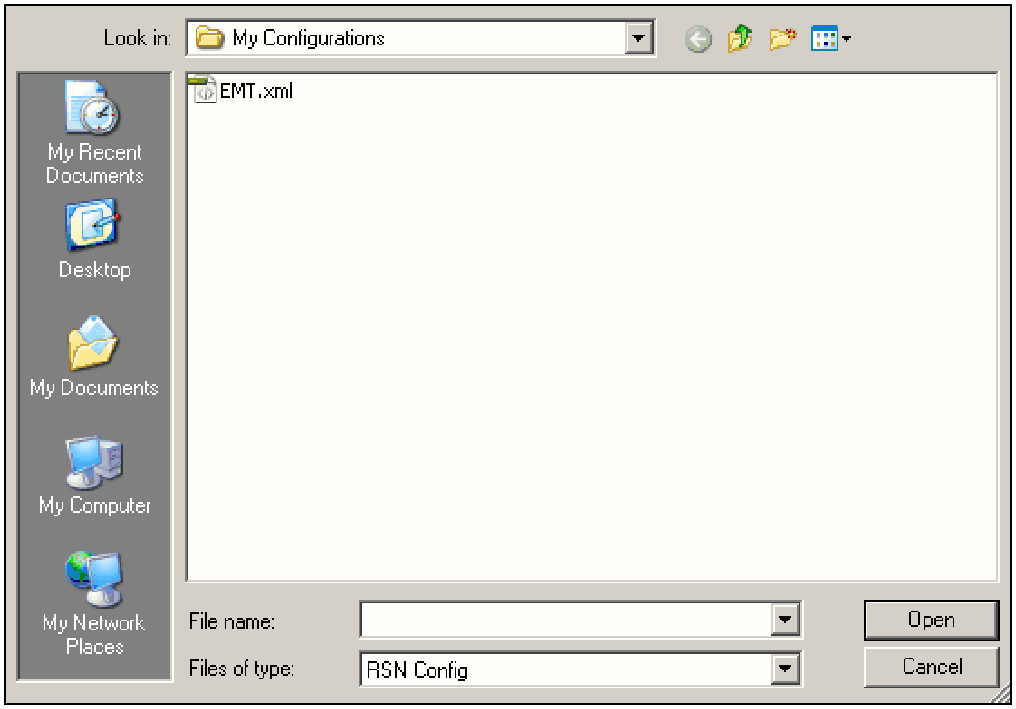
3. Browse to the folder location where you want to save this configuration.
4. Click **Save**.

The file is now exported as an XML file and can be imported into another RCT for use.

Import

To Import a configuration, do the following:

1. Select the parent configuration in the Configuration tree under which you want the import to appear.
2. From the **THC** file menu, select **Import Configuration**.



Look in: My Configurations

EMT.xml

File name:

Files of type: RSN Config

3. Select the file name to be imported and click **Open**.
   The configuration file is then automatically imported into the RCT and placed under the parent configuration you selected. If the configuration already exists, the imported configuration writes over the existing configuration, whether it resides under the parent configuration you selected or somewhere else in the configuration tree.

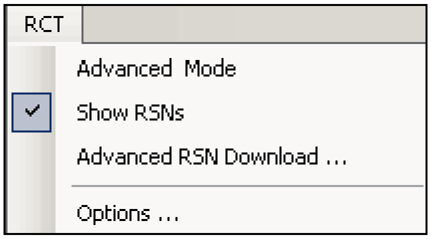
It is important to note that all values are overridden when importing a configuration. All imported parameters will be entered in an override state. A configuration can be re-inherited manually by re-entering individual parameters.

8.2.20 Additional RCT Menu Options Controlled by the TeraHop Console – User Role

File Menu

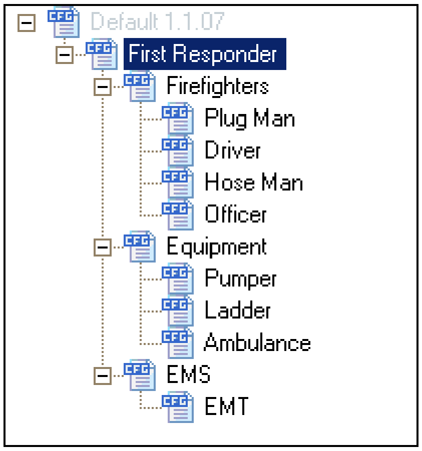
Logout allows you to log out of the application. Logging out of the application closes the RCT and takes you to the TeraHop Console.

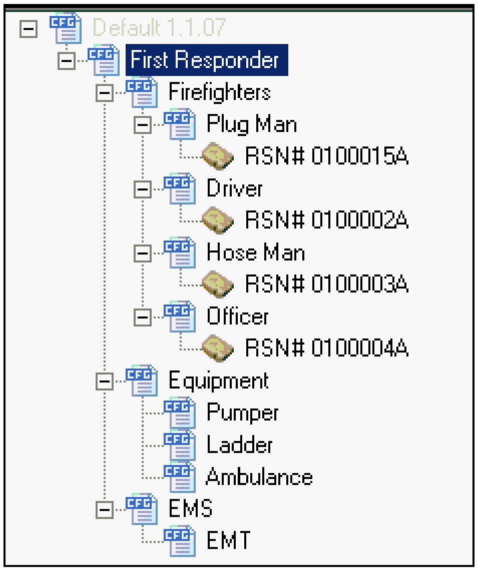
RCT Menu



Advanced Mode provides the same functionality as clicking the **Advanced Mode** button on the screen. See Advanced RCT Mode.

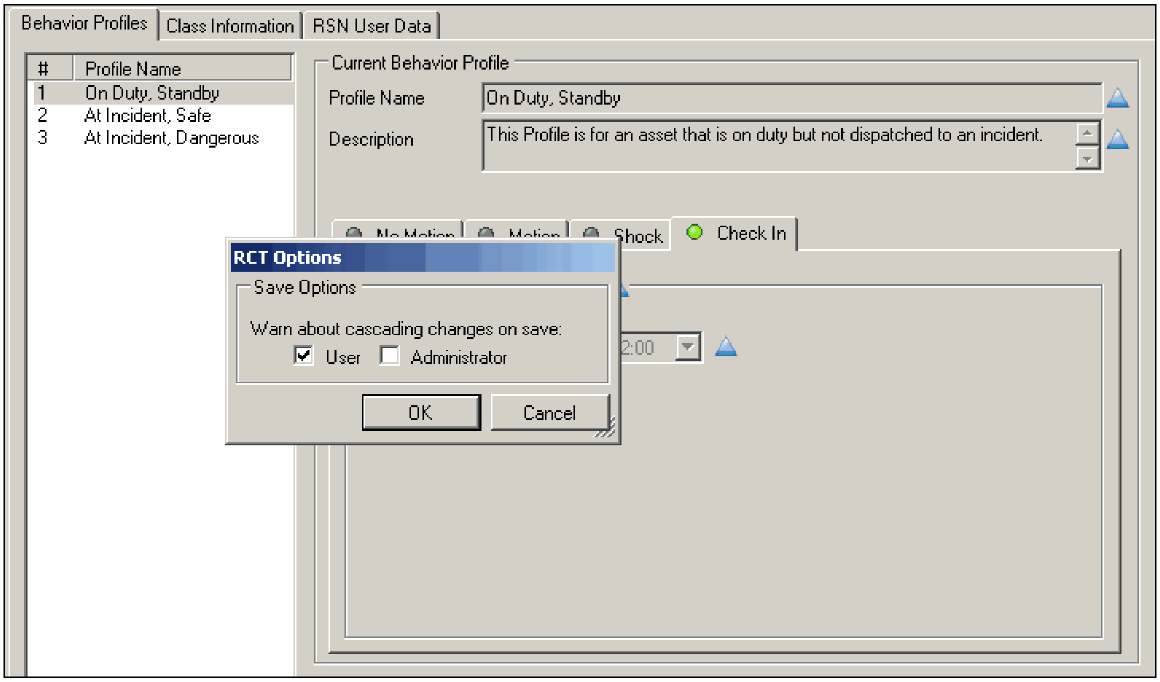
Show RSNs is a function that controls the display of the RSNs in the left-hand tree hierarchy. Enabling the option displays all of the associated RSNs. Disabling the option hides or collapses the RSNs under their associated configurations. This function can be useful if a large number of RSNs are displayed in the tree and you would like to collapse the display. The illustration on the left shows the Show RSN option disabled. The illustration on the right shows the Show RSN option enabled.





Advanced RSN Download launches the **RSN Direct Connect Downloader** screen so that advanced users can download RSN factory defaults, reset an RSN, power cycle an RSN, or place an RSN in sleep mode. See Downloading RSN Factory Defaults.

Options provides any user the ability to manage the display of Save warnings upon navigating away from a page which has been edited. You simply select the check box if this option is to be enabled.



#	Profile Name
1	On Duty, Standby
2	At Incident, Safe
3	At Incident, Dangerous

Current Behavior Profile

Profile Name: On Duty, Standby

Description: This Profile is for an asset that is on duty but not dispatched to an incident.

RCT Options

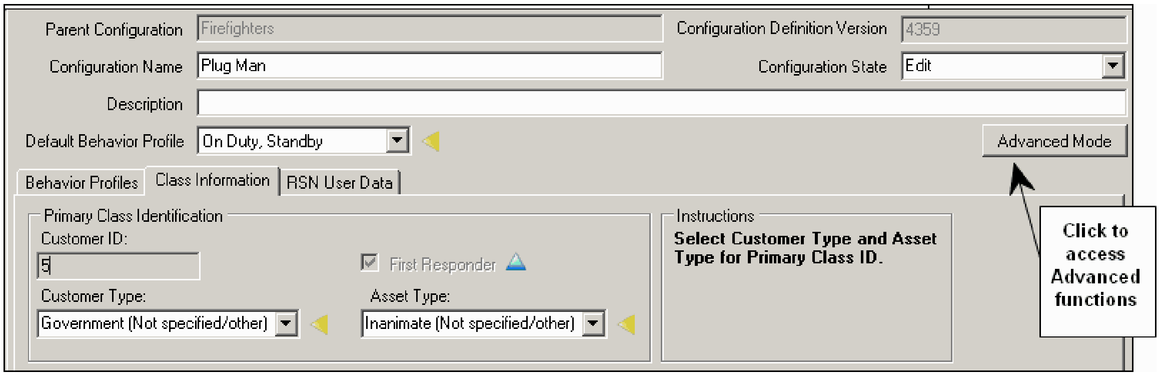
Save Options

Warn about cascading changes on save:

☑ User ☐ Administrator

8.2.21 RCT Advanced Mode

As discussed earlier, the application supports two user profiles: User role and Advanced role. The functionality described up to this point is accessible to either role. In addition to this functionality, the Advanced role has the ability to see more detailed sensor settings on the Behavior Profiles tab as well as configuring User Data fields.



Parent Configuration: Firefighters

Configuration Definition Version: 4359

Configuration Name: Plug Man

Configuration State: Edit

Description:

Default Behavior Profile: On Duty, Standby

Primary Class Identification

Customer ID: 5

☑ First Responder

Customer Type: Government (Not specified/other)

Asset Type: Inanimate (Not specified/other)

Instructions

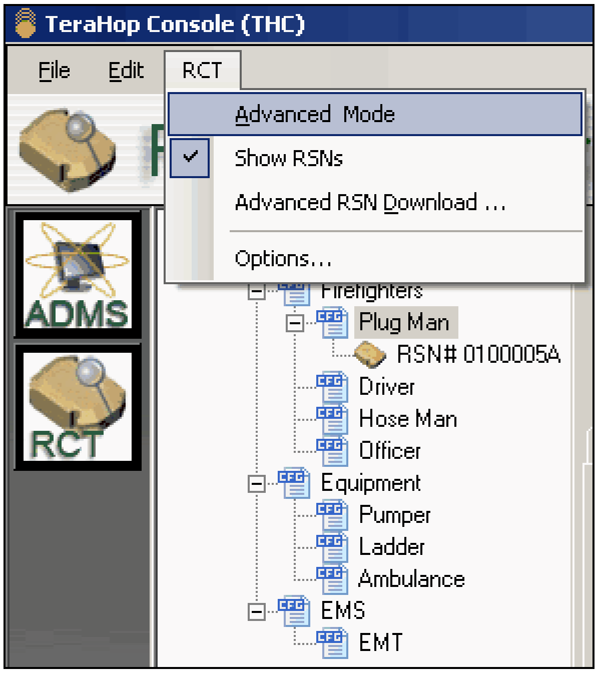
Select Customer Type and Asset Type for Primary Class ID.

Click to access Advanced functions

To access Advanced RCT functions, do the following:

1. If logged in as Advanced, in the upper right-hand corner of the screen click the **Advanced Mode** button.

2. To disable the advanced functions, click the **Advanced Mode** button again.
   You can also access the Advanced functions from the **RCT** menu on the top toolbar.



3. To access Advanced functions from the **RCT** menu, click the **RCT** menu and select **Advanced Mode**.

8.2.22 RSN User Data

8.2.22.1 What is RSN User Data?

The RSN provides a place to store data that can be viewed from the user application. This set of data is called the RSN User Data. The RSN and the Mobile Gateway System (MGS) do not use this data for any purpose; it is only of interest to the application.

Setup of user data elements is configured by the Advanced user. The application has access to RSN User Data as follows.

A portion of the User Data may be passed up to the application whenever an RSN is first registered to the network. This is called the registration user data set. It is configurable from the RCT. This is typically useful for a static set of data set in the RSN at time of configuration.

8.2.22.2 Usage Examples

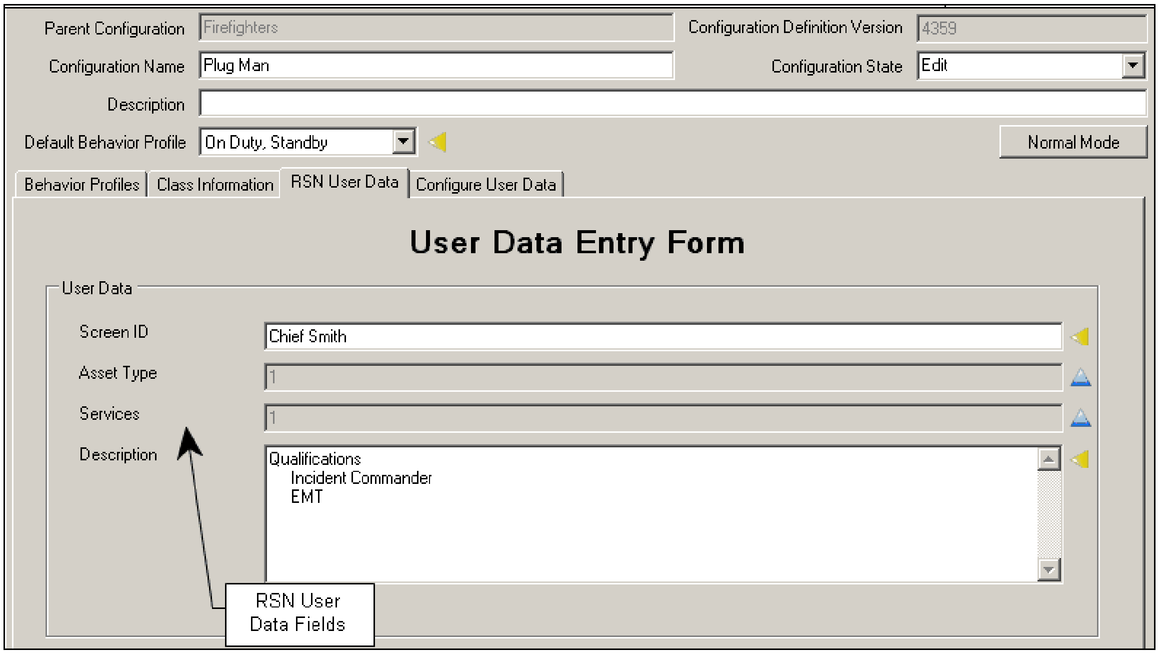
Examples of different kinds of user data might include:

- Asset identification
  This could be a complete descriptive set of information, or it might be a key data element that can be used to retrieve more information from an external database application.
- Asset Information
  This could be a large set of data. For instance it could be a qualifications of a First Responder wearing the RSN.

8.2.22.3 How User Data is Managed in the RCT

8.2.22.3.1 RSN User Data Entry Form

The RCT manages the RSN User Data in nearly the same manner as all other configuration parameters. The RSN User Data tab contains the User Data Entry Form. The user data elements on the form all have the same inheritance controls as other configuration parameters.



Parent Configuration: Firefighters
Configuration Definition Version: 4359
Configuration Name: Plug Man
Configuration State: Edit
Description:
Default Behavior Profile: On Duty, Standby

User Data Entry Form

User Data
Screen ID: Chief Smith
Asset Type: 1
Services: 1
Description:
Qualifications
    Incident Commander
    EMT

RSN User Data Fields

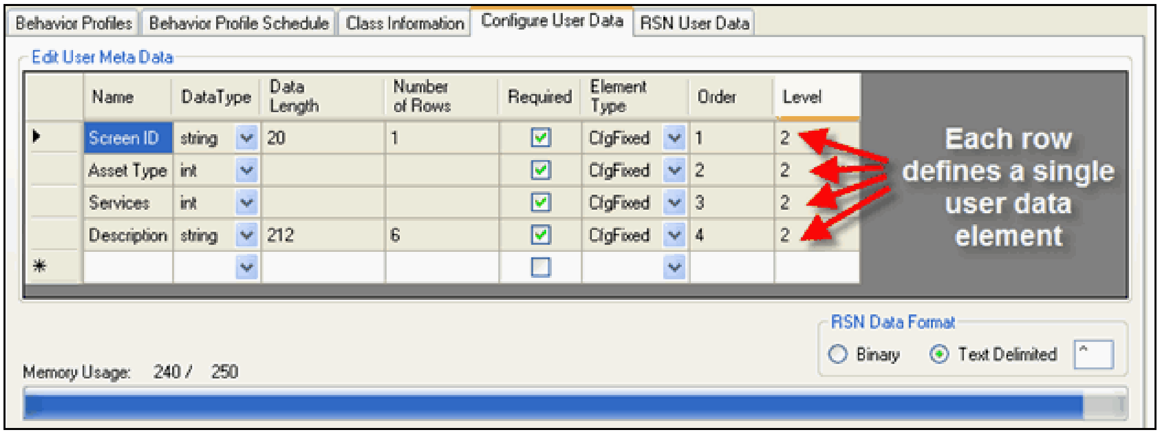
To ensure valid data entry, there are three forms of data validation:

- Required / not required – for a valid RSN level configuration
- Data Type validation (a string, an integer, a float, or a date-time field)
- String data types are validated for a maximum length

And actually, the field will stop accepting input when entry has reached its limit.

8.2.22.4 Configure User Data Form

RSN User Data elements must be defined in the RCT before they can be edited on a form. To define the RCT User Data elements, the RCT provides a Configure User Data tab with a table used to add, edit, and remove data element definitions.



	Name	DataType	Data Length	Number of Rows	Required	Element Type	Order	Level
▸	Screen ID	string	20	1	☑	CfgFixed	1	2
	Asset Type	int			☑	CfgFixed	2	2
	Services	int			☑	CfgFixed	3	2
	Description	string	212	6	☑	CfgFixed	4	2
*					□			

Each row defines a single user data element

RSN Data Format: ○ Binary ● Text Delimited ^

Memory Usage: 240 / 250

Figure 21: Configure User Data Form

An RCT User Data element definition consists of

- An element name
  This becomes the field label on the RSN User Data form.
- A data type
  This is used to validate what are allowable values and to indicate how the data is stored in the user data block.
  There are three types:
- String – any set of characters and stored as a fixed length set of characters as defined by the data length
- Int. – an 4 byte integer value
- Float – a 5 byte floating point value
- Data Length
  This is only relevant for elements of data type equal to string. This specifies the length of the string. It is necessary to control the space allocated in the user data for this string data element.
- Number of Rows
  This informs the user data entry form how many rows should be displayed for this field. It is mainly useful for longer string data elements that may need multiple lines of entry.
- Required
  This indicates if this field is required. This affects validation on the User Data Entry form. A required field must have an entry before a RSN level configuration can be saved.

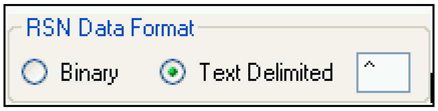
- Element Type
  This value indicates how the field is handled by the RCT. A value of CfgFixed is the only value that affects the RCT. This value places this data element in the Registered User Data set to be uploaded to the application during a RSN registration event.
- Level and Order – Not Editable
  These fields are used to order the fields in the user data block. The order of the table is first level and then order.

  In addition, the level field indicates at which level of the inheritance tree the element is defined. A value of 1 indicates that this user data element row is defined at the current configuration level. A value of 2 indicates that this user data element row is defined at the parent of the current configuration level and other values reflect higher levels up the tree.

Editing the element definitions is straightforward table editing.

- To Insert a new user data element, enter definition values for it on the bottom line.
- To Delete a user data element, select the row and then press the delete key
- To Edit a user data element, select the cell and change its value

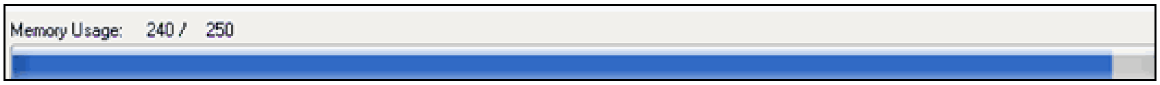
Once all user data element edits are complete, click the Save Configuration button. Saving the edits will reconstruct the RSN User Data Entry Form accordingly.


RSN Data Format

○ Binary ● Text Delimited ^

The RSN Data Format dictates the method that these user data elements are packed into the user data memory block on the RSN.

- Binary
  The user data is converted to binary representation and packed in to memory with no alignment gaps.
- Text Delimited
  The user data elements are converted to one long string with the specified field delimiter used to separate element values.


Memory Usage: 240 / 250

The memory bar shown indicates how much of the available user data space is filled up by the user data elements defined in the table above. There is a limit of 250 bytes and if the user data extends beyond that size limit, then the bar will go “Red” to indicate an overwrite situation.

Inheritance Special Note

User data elements can be specified in different branches of the inheritance tree. User data elements defined in child configurations append to the user data elements defined in parent configurations. Editing of user data element definitions can only occur in the configuration they were defined. There is no OVERRIDE option for User data element definitions.

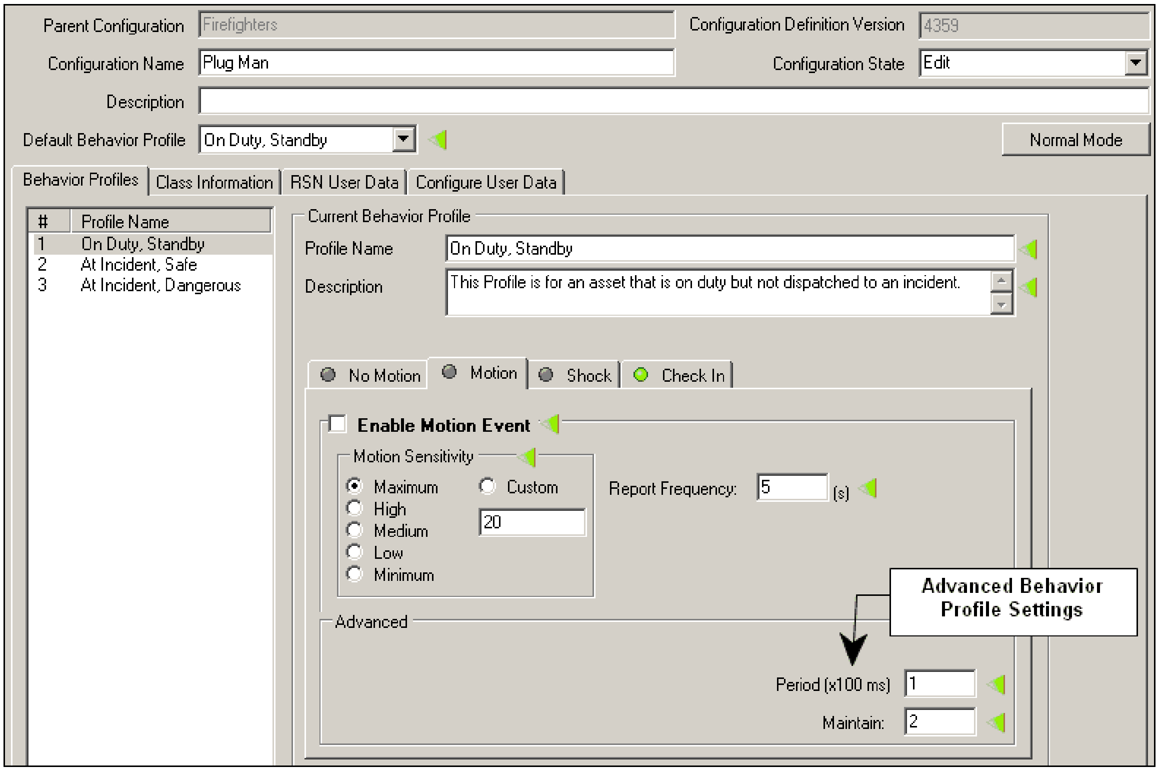
Notice that the table editor will block editing of parent-defined rows.

Import / Export Special Note

When exporting a configuration with user data element, the exported file only contains user data element definitions which are defined for its level in the hierarchy. By doing it this way, exporting and then re-importing will not create duplicate entries for the parent elements.

Behavior Profiles

The parameters defined here are specific for each sensor and need to be configured as such. To access these settings, click a Behavior Profile tab. The Advanced Functions appear at the bottom of the section in an area labeled Advanced. They are described in the table on the next page.



Parent Configuration: Firefighters
Configuration Definition Version: 4359
Configuration Name: Plug Man
Configuration State: Edit
Description:
Default Behavior Profile: On Duty, Standby

#	Profile Name
1	On Duty, Standby
2	At Incident, Safe
3	At Incident, Dangerous

Current Behavior Profile
Profile Name: On Duty, Standby
Description: This Profile is for an asset that is on duty but not dispatched to an incident.

☐ Enable Motion Event

Motion Sensitivity
● Maximum
○ High
○ Medium
○ Low
○ Minimum
○ Custom 20

Report Frequency: 5 (s)

Advanced
Period (x100 ms) 1
Maintain: 2

Parameter	Description
Period	How frequently the RSN checks for the defined condition. It is recommended the default value not be changed unless a specific application or field experience determines a different frequency is required. The sample time is in 100 ms increments.
Maintain	The number of consecutive samples the threshold must be exceeded to generate an event. It is recommended that the default value not be changed unless a specific application or field experience determines a different sample rate is required. Multiplying these two numbers ((P value x 100 ms) * M = event trigger) calculates the timing for the triggering event. For example, a Period of 10 and a Maintain of 5 provides an event trigger time of 5000 ms or 5 seconds.

Alternatively, there is an advanced download window that is available to an Advanced User. From the **RCT** menu, select **Advanced RSN Download**.

Note: You can also download user configurations from the RSN Direct Connect Downloader screen.

8.2.23 Downloading RSN Factory Defaults

This feature is only available to RCT Advanced users.

Using the RSN Configuration Tool (RCT) and the RCT Cradle, if necessary, you can download the factory defaults for an RSN.

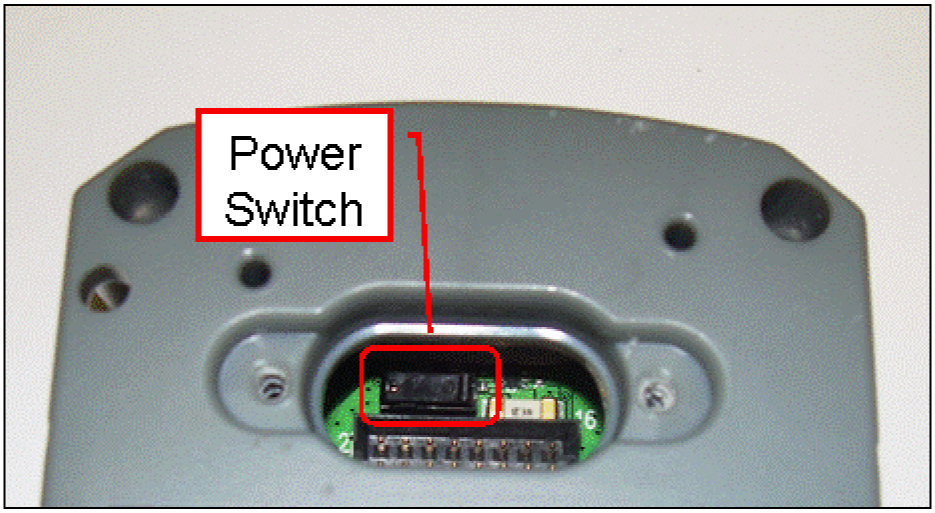
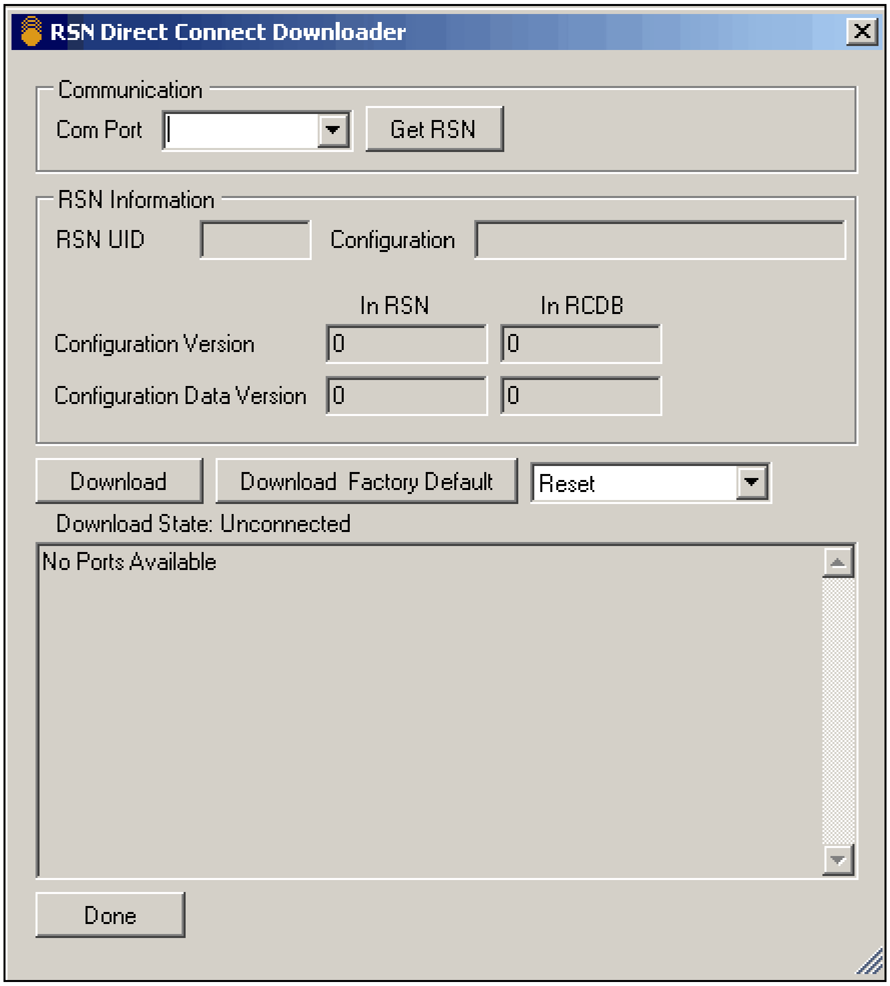


Figure 22: Power Switch on RSN

In the RCT, to download RSN factory defaults, do the following:

1. Remove the plug from the back of the RSN.
2. Place the RSN in the RCT Cradle.
3. Click the **Advanced** button, if necessary.
4. From the **RCT** menu in the top toolbar, select **Advanced RSN Download**.
   The **RSN Direct Connect Downloader** window opens.
   Notice that the **Download** button and **Get RSN** button work the same as they do on the main RCT screen in the lower left corner.



	In RSN	In RCDB
Configuration Version	0	0
Configuration Data Version	0	0

Reset

Download State: Unconnected

No Ports Available

5. Under **Communication**, click the **Com Port** drop-down arrow and select the port to which the RCT Cradle USB cable is connected.
6. Click **Get RSN**.
7. Verify the **RSN UID** is the same as the label on the RSN.
8. In the **Reset** field next to the **Download Factory Default** button, click the drop-down arrow and select one of the following:

Reset - to reboot the RSN. Do this when you want to use the RSN. If you reset the RSN, it will not appear on a network until you download a configuration to it.

Sleep - sleep mode. Use this when you want to put the RSN on a shelf for future use. When you want to use the RSN, you will need to awaken it. See How to Wake Up or Troubleshoot an RSN.

Shutdown - Shut down (power cycle) - turn the RSN off. Use this when you want to turn off the power to the RSN by depressing the black power switch inside the RSN plug cavity (see illustration below) for several seconds and then releasing it. Power cycling the RSN takes the RSN out of service. To recover, hold the power switch down for several seconds and then release it.

9. Click **Download Factory Default**.
   The RSN has been set to its factory defaults, and depending on your selection, is either in deep sleep, has been reset, or has been shut down.
10. Remove the RSN from the RCT Cradle and insert the plug cover using the plug cover screws.

8.3 Configuring RSNs for the TeraHop IMS Application

8.3.1 Configuring RSNs for the TeraHop IMS Application

The following instructions describe how to configure RSNs specifically for use with the TeraHop Incident Management System *with* Automated Accountability application, called the IMS for short. RSNs are configured using the TeraHop RSN Configuration Tool (RCT) software. The RCT is accessed from the TeraHop Console on a laptop computer.

Before using these instructions, please read and understand the concepts and use of the RSN Configuration Tool (RCT) and planning RSN configurations in the section titled Configuring RSNs with the RSN Configuration Tool. It is important to have a thorough knowledge of the RCT concepts and design before attempting to configure an RSN.

RSNs that are used with the IMS are shipped from the factory to the Channel Partner preloaded with RSN firmware and default configurations. You still need to configure the RSN with additional information. Once the planned configuration tree structure is designed, create it in the RCT. You will then go to each configuration level and select the appropriate parameters and settings to be associated with the corresponding configuration. For details on how to configure an RSN, see Configuring RSNs with the RSN Configuration Tool.

The basic steps for configuring an RSN for use with the IMS are:

- Plan your configurations. Determine how the agency RSNs will inherit the properties of the configuration above it.
  In the RCT, do the following:
- Create the configuration tree for the agency.
- Associate each RSN with a configuration.
- Set the parameters for the RSN Sensors.
- Set the Class Information.
- Set the Customer Type.
- Enter User Data for each RSN.
- Download the configuration to the RSN.

8.3.2 Plan Your Configurations

For the First Responder market, TeraHop Networks recommends that you plan your configurations as follows:

First Responder RSN Default Configurations

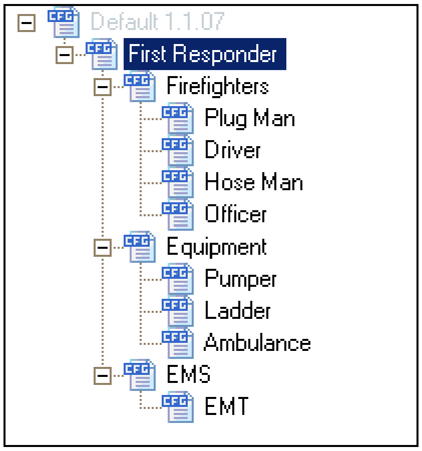
For the First Responder market, the RCT supports three Behavior Profiles and comes provided with three default configurations:

- On Duty, Standby is typically used for an asset that is on duty but not dispatched to an incident.
- At Incident, Safe is for an asset which is on scene of an incident but not in a dangerous or life-threatening assignment.
- At Incident, Dangerous is for an asset which is on the scene of an incident and is in a dangerous or life-threatening assignment.

The Profile within an RSN will not change unless configured to do so through a condition experienced in the field or through a command given through a user application.

8.3.3 Create the Inheritance Tree

For the First Responder market, TeraHop Networks recommends that you create the inheritance tree similar to the tree illustrated below.



- Default 1.1.07
  - First Responder
    - Firefighters
      - Plug Man
      - Driver
      - Hose Man
      - Officer
    - Equipment
      - Pumper
      - Ladder
      - Ambulance
    - EMS
      - EMT

8.3.4 Associate Each RSN with a Configuration

After you have created the inheritance tree in the left-hand pane, you need to associate each RSN with a configuration.

See the instructions in Configuring RSNs with the RSN Configuration Tool (RCT), Associating RSNs with Configurations.

8.3.5 Set the Parameters for the RSN Sensors

Recommended settings for Motion, No Motion, Shock sensors and Check-in.

For each RSN now in your configuration tree, you need to set the parameters of the RSN sensors.

The key parameters that can be configured through the Behavior Profiles are the enabling or disabling of supported sensors (No-motion, Motion, and Shock) and the RSN Check-in rate.

- No-motion is a sensor that detects whether the asset the RSN is attached to has stopped moving for a specified duration. For example, should a First Responder become disabled and remain motionless for a defined period of time, the RSN will issue an alarm to you application to this effect.
- Motion is a sensor that detects whether the asset the RSN is attached to is moving at a level and time that it should not be. For example, if an RSN is attached to a piece of stationary equipment that suddenly begins moving, the RSN will issue an alarm to you application to this effect.
- Shock is a sensor that when the RSN is struck with a pre-configured force, the RSN will issue a distress alarm to you application to this effect.
- The RSN Check-in time is the elapsed time between when the RSN checks in with the TeraHop network to confirm network connectivity. This is defined for each Profile. For example, an asset assigned to a dangerous task would want a more frequent check-in than an asset in rehab.

It is important to note that the internal sensors are mutually exclusive. That is, an RSN cannot have both Shock and Motion enabled at the same time.

Although the Tool supports three profiles, only one profile is active at a time, meaning that its sensory monitoring and reporting settings are the ones that the RSN is following. All other profiles are dormant until initiated by your application, or a pre-determined field condition is experienced.

8.3.6 Set the Class Information

The Class Information is used to define the TeraHop network with which the configured RSNs can communicate, whether it is a TeraHop network generated by the organization configuring the RSNs, or one that is joined in a merge or mutual aide scenario. As the defaults are already set for the First Responder market, no changes to the parameters defined under this tab should be required unless the RSN Asset Type is to be associated with a piece of equipment rather than an individual.

To edit the Asset Type parameter on the Class Information tab, do the following:

1. In the configuration tree, select the configuration.
2. Override the default for the **Asset Type** field.
3. In the **Asset Type** field, click the drop-down arrow and select **Inanimate**.

8.3.7 Set the Customer Type

As the defaults are already set for the First Responder market, no changes to the parameters defined under this tab should be required unless the Customer Type is a commercial entity and not Government.

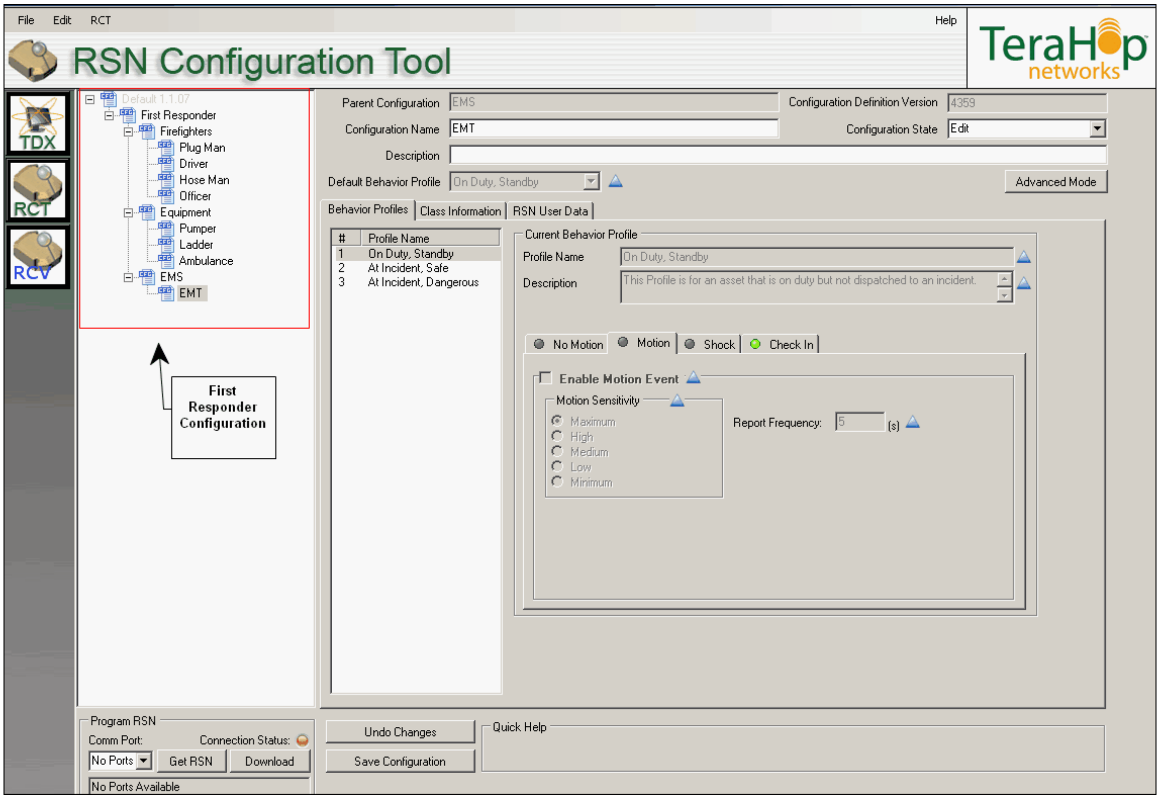
Should the configuration be for a commercial entity, do the following:

1. Click the Class Information tab.
2. Override the default for the **Customer Type** field.
3. In the **Customer Type** field, click the drop-down arrow and select **Commercial**.
4. Click the **Save Configuration** button at the bottom of the Middle section of the screen. The Customer ID is a fixed number assigned by TeraHop Networks and cannot be edited from this screen.

8.3.8 Enter the Customer User Data

The last configurable parameter is the **Customer User Data**. This data is a block of memory on the RSN that is available for the application to use as desired. In our First Responder example, there are four data fields in this area that are configured based on you application specifications. In the First Responder example used throughout these sections, the fields are for screen name, asset type, service type, and a free-form text description. This may include specifications about a piece of equipment or specific qualifications of an individual. This data is what is passed on to your application when an asset is accessed.

The following example shows how a typical First Responder configuration may be set up. The left-hand panel is always where configurations and RSN assignments are defined.



Parent Configuration: EMS

Configuration Definition Version: 4359

Configuration Name: EMT

Configuration State: Edit

Description:

Default Behavior Profile: On Duty, Standby

#	Profile Name
1	On Duty, Standby
2	At Incident, Safe
3	At Incident, Dangerous

Current Behavior Profile

Profile Name: On Duty, Standby

Description: This Profile is for an asset that is on duty but not dispatched to an incident.

☐ Enable Motion Event

Motion Sensitivity: ● Maximum ○ High ○ Medium ○ Low ○ Minimum

Report Frequency: 5 [s]

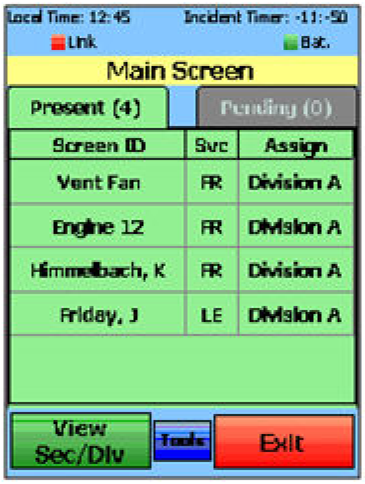
Comm Port: No Ports

No Ports Available

Once the RSN is selected and assigned, you can then enter the RSN’s user data from the RSN User Data tab.

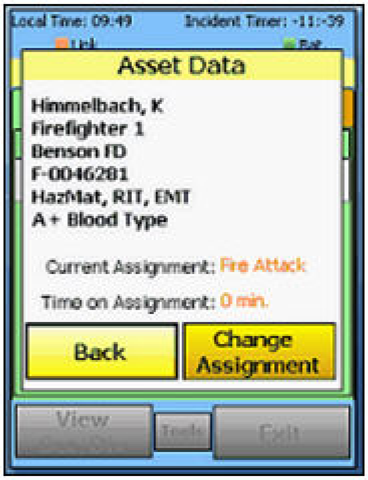
In the IMS application, static user data is used to hold identifying information about the asset assigned to the RSN. These data are presented on the Incident Commander's (IC's) PDA to inform the IC about the asset. In the Present and Pending lists, the asset's Screen ID is presented. When an asset's Screen ID label is double-tapped, the asset's Asset Data pop-up window opens, displaying additional data about that asset. Refer to the examples below.

Present List on PDA



Screen ID	Svc	Assign
Vent Fan	FR	Division A
Engine 12	FR	Division A
Himmelbach, K	FR	Division A
Friday, J	LE	Division A

Asset Data Popup on PDA



Himmelbach, K
Firefighter 1
Benson FD
F-0046281
HazMat, RIT, EMT
A+ Blood Type

Current Assignment: Fire Attack

Time on Assignment: 0 min.

The popup contains the screen Id, the asset type, the service type, and a text description of the asset.

The IMS application receives this user data as User Data upon registration. Using data in this manner affords the application the ability to not utilize a database of RSN to Asset description database.

This approach has moved the database of RSN to Asset information to the RCT Database. This information is setup and managed in the RCT Database.

User Data Entry Form

The RCT provides you with access to a block of memory within the RSN to enter specific data. RSN user data allows RSNs to be programmed with customer-specific descriptive data. The data that is placed in this area is for information only and is what is displayed on your application when an RSN is displayed.

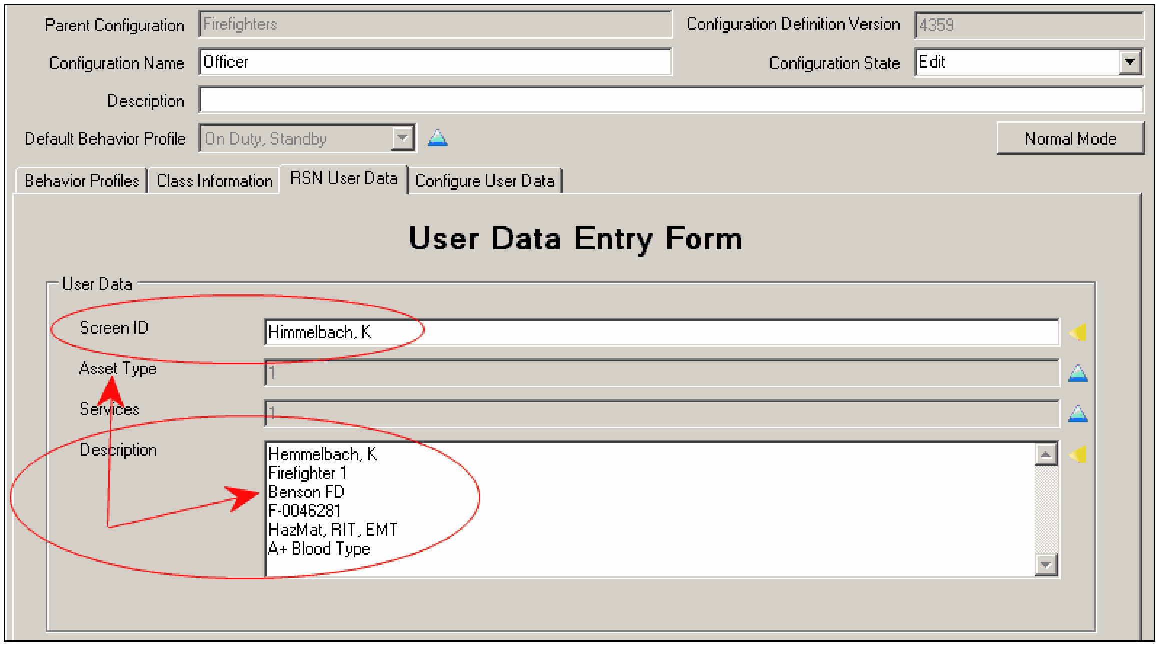
To edit each of these fields, select the Override option and enter the desired information into the data field using the information in the table below.

Field	Data to Enter
Screen ID	Typically the name assigned to the RSN, such as Chief Smith or Engine 42. The way the data is entered and formatted into this field is how it will be displayed within your application.
Asset Type	The entry is either 1 or 2, with 1 being for a Human and 2 being for an Inanimate object such as a piece of equipment. This value must be

Field	Data to Enter
	consistent with that selected under the Class Information Asset Type.
Services Setting	The Service setting is displayed on the screen of the application and is applicable to a specific user application. The following list identifies the various options for this field. Enter the number for their corresponding description. For our First Responder example, we are using firefighters, and therefore a 1 should be entered. 1 Fire, Rescue 2 Police, Law 3 EMS, Ambulance 4 Utilities 5 Mayor, Admin 6 Military 7 Visitor 8 Other
Description	A free-form data entry field where any applicable information about the person or equipment carrying the RSN can be added. This may include specifications about a piece of equipment or specific qualifications of an individual. The Tool provides this capability for download at the RSN configuration time.

You should check the IMS application configuration to ensure consistency between the two systems.

Below is an illustration of the User Data Entry Form screen for the User Data block. The data are typed in, per the formats that follow, further below.



Parent Configuration: Firefighters

Configuration Definition Version: 4359

Configuration Name: Officer

Configuration State: Edit

Description:

Default Behavior Profile: On Duty, Standby

User Data Entry Form

User Data

Screen ID: Himmelbach, K

Asset Type: 1

Services: 1

Description:
Hemmelbach, K
Firefighter 1
Benson FD
F-0046281
HazMat, RIT, EMT
A+ Blood Type

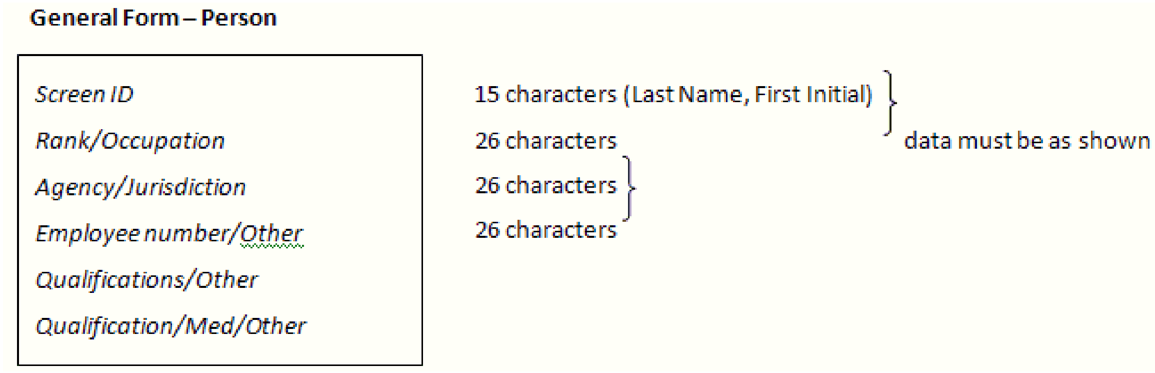
Entering User Data

User Data are typed in as indicated on the illustration of the RCT (previous page). There is a specific order, and there are space limits that must be observed for the User Data to assure that the data are readable when presented on the Present and Pending lists and in the Asset Data popup on the PDA. Observing the order also assures consistency within each individual agency and among agencies of a mutual-aid group. The consistency assures that the data are found and understood quickly and correctly, regardless of which company's, precinct's, or agency's assets are being monitored at an incident.

Screen ID is key. It identifies the asset to the Incident Commander (IC). It is used in several places, and it must fit within in the space available on the PDA. The term "Screen ID" is used since it may apply to any asset type, regardless whether a person, Unit, vehicle, etc. (as opposed to "Name," which would apply only to people). Screen ID is limited to 15 characters (including spaces & punctuation).

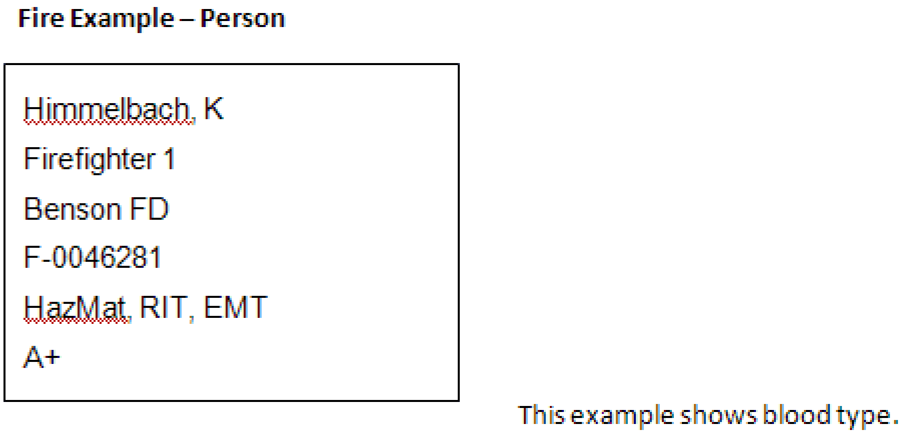
Conform to the following formats when entering in User Data in the RCT. It is recommended that all assets be identified and that the User Data of each be planned and prepared before using the RCT.

The following are recommended formats for RSNs assigned to people.



General Form – Person

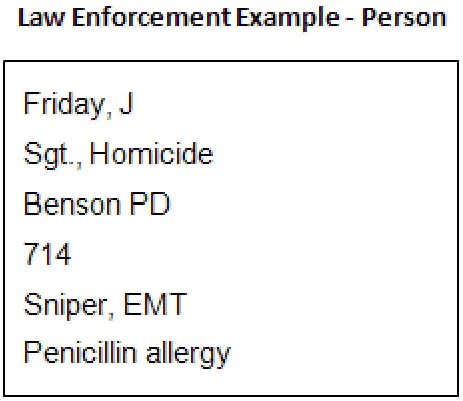
Screen ID	15 characters (Last Name, First Initial)	data must be as shown
Rank/Occupation	26 characters	
Agency/Jurisdiction	26 characters	
Employee number/Other	26 characters	
Qualifications/Other		
Qualification/Med/Other		



Fire Example – Person

Himmelbach, K
Firefighter 1
Benson FD
F-0046281
HazMat, RIT, EMT
A+

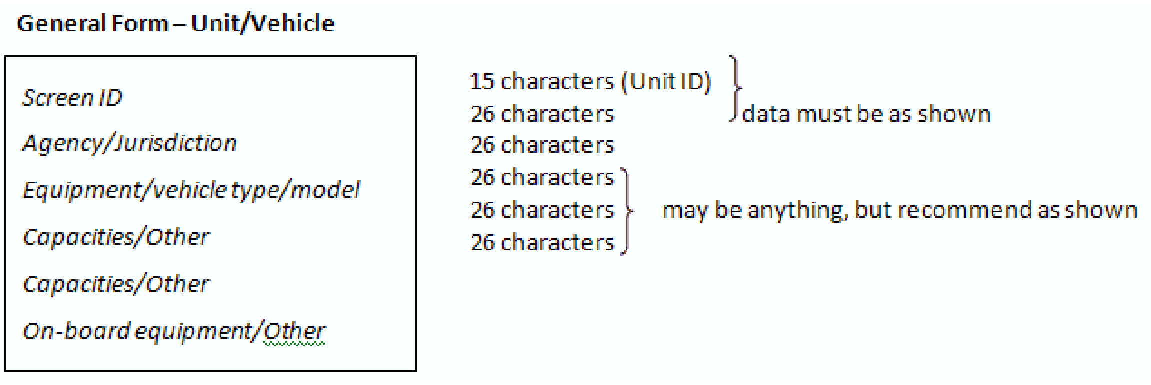
This example shows blood type.



Law Enforcement Example - Person

Friday, J
Sgt., Homicide
Benson PD
714
Sniper, EMT
Penicillin allergy

The following are recommended formats for RSNs assigned to units/vehicles.



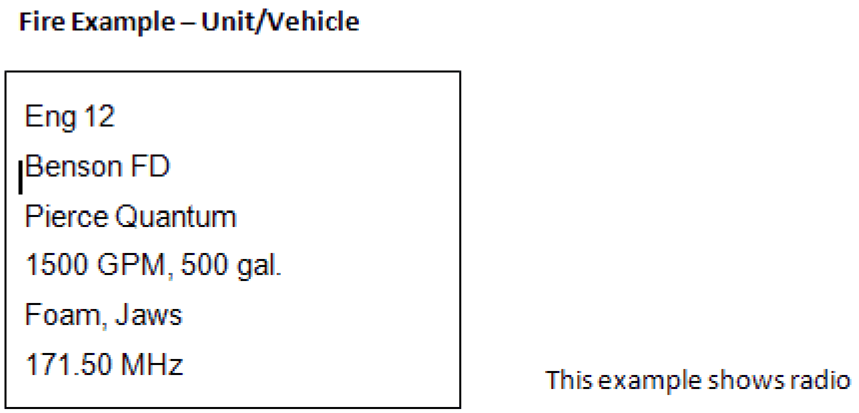
General Form – Unit/Vehicle

Screen ID
Agency/Jurisdiction
Equipment/vehicle type/model
Capacities/Other
Capacities/Other
On-board equipment/Other

15 characters (Unit ID)
26 characters
26 characters
26 characters
26 characters
26 characters

data must be as shown

may be anything, but recommend as shown

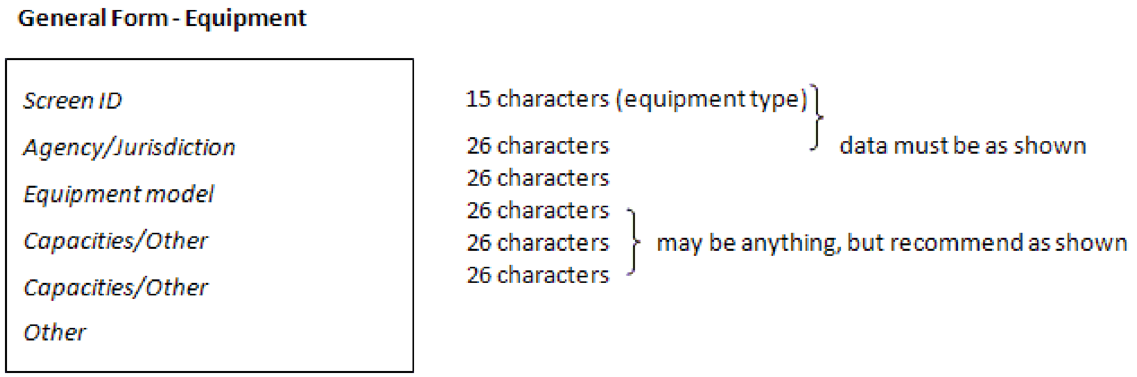


Fire Example – Unit/Vehicle

Eng 12
Benson FD
Pierce Quantum
1500 GPM, 500 gal.
Foam, Jaws
171.50 MHz

This example shows radio

The following are recommended formats for RSNs assigned to equipment.



General Form - Equipment

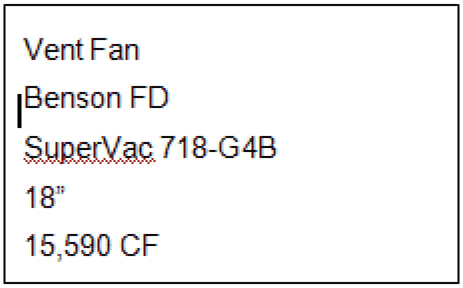
Screen ID
Agency/Jurisdiction
Equipment model
Capacities/Other
Capacities/Other
Other

15 characters (equipment type)
26 characters
26 characters
26 characters
26 characters
26 characters

data must be as shown

may be anything, but recommend as shown

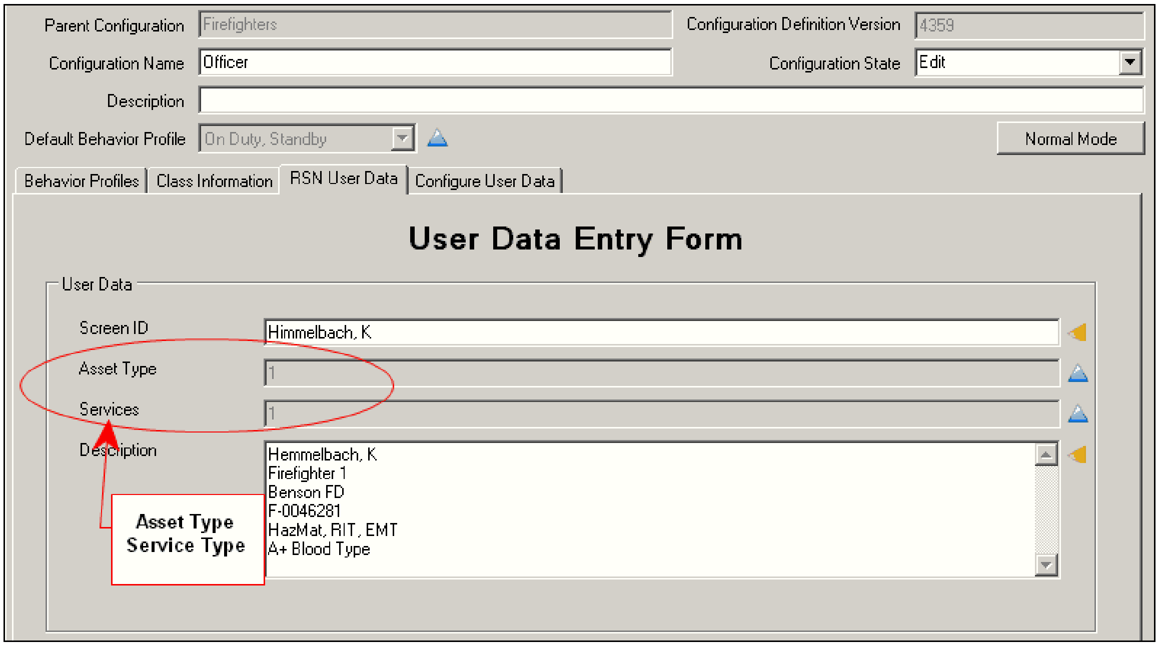
Fire Example - Equipment



Vent Fan
Benson FD
SuperVac 718-G4B
18"
15,590 CF

Other User Data to Configure

There are two additional user-data items that need to be configured using the RCT. Both are configured on the same screen as the User Data block.



Parent Configuration	Firefighters	Configuration Definition Version	4359
Configuration Name	Officer	Configuration State	Edit
Description			
Default Behavior Profile	On Duty, Standby		

User Data Entry Form

User Data

Screen ID	Himmelbach, K
Asset Type	1
Services	1
Description	Hemmelbach, K Firefighter 1 Benson FD F-0046281 HazMat, RIT, EMT A+ Blood Type

Asset Type
Service Type

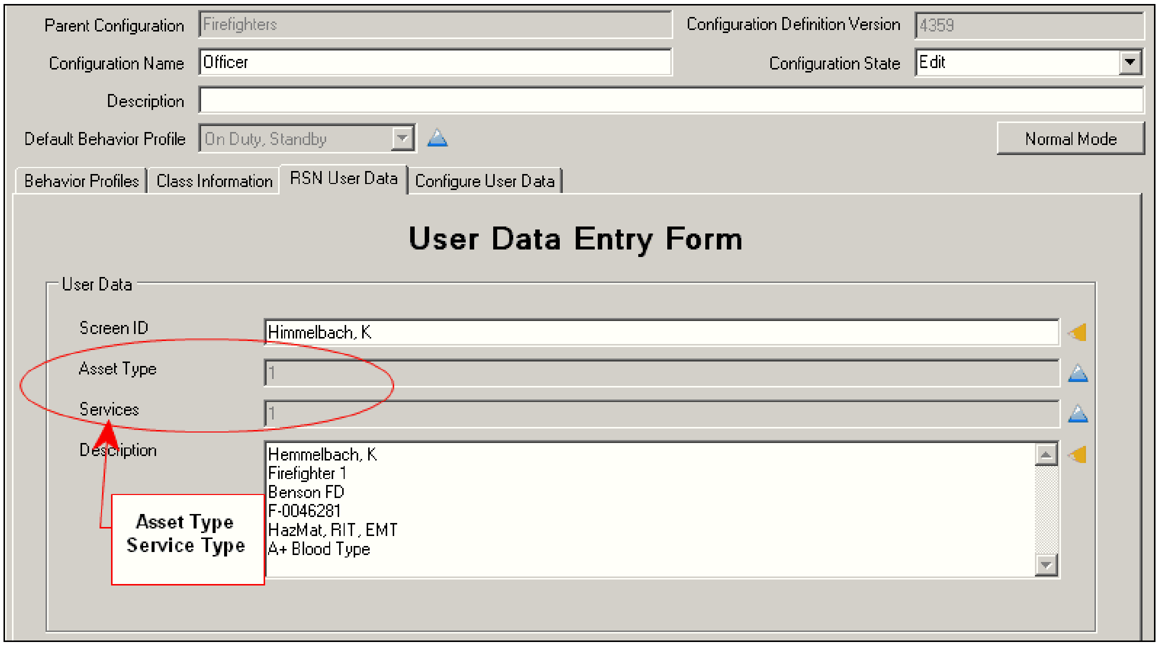
Asset Type is a numerical reference that the IMS uses to identify the kind of asset to which an RSN is attached. The IMS PDA displays data differently depending on whether an asset is a person, or Unit/vehicle, etc. The choices for Asset Type that are available in the RCT are:

Ref. #	Corresponding Asset Type
1	Individual person
2	Commander
3	Unit/vehicle
4	Equipment (not associated with a Unit)
5	K9

Service Type is another numerical reference that the IMS uses to identify the kind of service of the asset to which an RSN is attached. The IMS PDA displays a 2-letter indicator of an asset's service type to enable the IC to quickly identify and sort all assets of a give service type. For example, and IC may wish to identify all assets on-scene that are law enforcement, and do so quickly. The choices for Service Type that are available in the RCT are:

Reference Number	Description	Application Screen Label
1	Fire, rescue	FR
2	Police, sheriff, DA	LE
3	EMS, ambulance, medical	EM
4	Utilities and roads	PW
5	Public Health	PH
6	Military	ML
7	Visitor	V
8	Administration and Other	A/O

The illustration below shows where Asset Type and Service Type are configured in the RCT.



Parent Configuration: Firefighters

Configuration Definition Version: 4359

Configuration Name: Officer

Configuration State: Edit

Description:

Default Behavior Profile: On Duty, Standby

User Data Entry Form

User Data

Screen ID: Himmelbach, K

Asset Type: 1

Services: 1

Description:
Hemmelbach, K
Firefighter 1
Benson FD
F-0046281
HazMat, RIT, EMT
A+ Blood Type

9.0 Operational Checkout and System Commissioning

9.1 Operational Checkout

The following procedure can be used to verify that the system has been installed properly and that it is operational following field installation and/or a corrective action, such as replacement of a system component.

This procedure is divided into two parts; first, is a visual inspection that can be performed prior to turning the system on; and second, is a step-by-step procedure that shall be performed to ensure the system is fully operational. Troubleshooting is embedded within the body of this procedure.

9.1.1 Visual Inspection

The following should be checked visually. If you notice defects, immediately notify the installer and have each issue resolved.

1. If structural holes were drilled to pass cable, check the following:
   - Make certain that the insulation on all cables is intact, with no cracks or abrasions. Ensure that no bare wire is exposed, and that no dielectric material is exposed.
   - Make certain a rubber grommet has been installed in every hole drilled through metal. This will prevent future damage to the cables passing through these holes.
   - Make certain that a silicon sealant has been applied to every location that a cable passes through the exterior of the vehicle. This will prevent water ingress.
   - Equipment mounted inside the vehicle should be positioned such that a minimal amount of cabling has to be used, particularly for powering.
2. Cables that originate outside should be routed in as professional manner as possible. Full use shall be made of headlines and channels within the vehicle to conceal cables as much as practical. Check the following wiring:
   - From the Garrett Ethernet switch (RJ45 connectors), make the following connections:
   - To the Ethernet connection on the Gateway Router. If mounted outdoors, verify connection is shielded for outdoor use
   - To the top left Ethernet connection on the Gateway Server (near the DB-9 connector)
   - To the top left Ethernet connection on the MMR System (near the DB-9 connector).

3. Trace the DC input from the source (battery) and check the following:
   - That a 12VDC Input from the source (12VDC Automotive Battery) is being applied to the High Current System ON/OFF Switch, and the High Current Barrier Strip. Verify the following
     - 10AWG wire is used between the battery and the high-current barrier strip
     - 10AWG wire is used between the high-current barrier strip and the distribution barrier strip.
4. Verify that 22AWG wire (Positive and Negative) is routed from the barrier strip to the Garrett Ethernet Switch.
5. Verify that positive and negative 18AWG wire is routed from the barrier strip to the DC input of the Gateway Router. If mounted outdoors, ensure power connection is shielded for outdoor use.
6. Verify that positive and negative 18AWG wire is routed from the barrier strip to the DC input of the MMR System.
7. Verify that positive and negative 18AWG wire is routed from the barrier strip to the DC input of the Gateway Server.

9.2 System Operation

The following procedure is provided to allow the installer/operator to verify proper system operation in a simple straightforward manner. Troubleshooting is included within the body of this procedure. When reading the procedure you will notice information within a heavily bordered box. This information is applicable only when the operator does not get the desired result at a given step. In these instances, the operator shall adhere to the information within the bordered area. When the resulting actions are complete the operator shall continue performance of the steps outside the bordered area. Information within these borders shall be ignored as long as the desired result for each step is taking place.

1. Power up the system by placing the high-current system on/off switch to the **On** position.
2. The GW Router will power up. At the time of printing this document, the only way to confirm power to the GW router is by connecting a laptop to the Ethernet switch and “pinging” the GW Router. Installations that take place in the near future will include a new GW Router that has a group of indicators on the bottom of the unit. The PWR indicator can be observed in order to verify that power is applied to the GW Router.
3. Is the GW Router the only DC powered device that is not powered up? Troubleshoot the wiring between the DC power supply and the GW Router and, if necessary, make wiring repairs. Otherwise replace the GW Router.

   The GW Server will be powered up. Power to the GW Server can be confirmed by the illumination of the red LED on the back of the device and the green Ethernet connector LED.

4. Troubleshoot the wiring between the DC power supply and the GW Server and, if necessary, make wiring repairs. Otherwise replace the GW Server.

   The MMR System will be powered up. Power to the MMR System can be confirmed by the illumination of the red LED on the back of the device and the green Ethernet connector LED.

5. Troubleshoot the wiring between the DC power supply and the MMR System and, if necessary, make wiring repairs. Otherwise replace the MMR System.

   The Ethernet Switch will be powered up. The switch is equipped with an indicator that indicates when power is applied. The switch should also illuminate a single indicator for each device that is connected to it.

6. Troubleshoot the wiring between the power strip and the Ethernet switch. Check for DC voltage at the power input of the Ethernet switch. If power is present, replace the switch. If power is not present, power is not being routed from the power strip to the switch; repair wiring issues.

   About three minutes after system power up, the system can start an incident on the PDA.

7. Place a few RSNs in the area.
8. Power up the PDA.
   Observe the First Responder Accountability screen.
9. If the screen does not appear, replace the battery in the PDA.
10. If this action does not solve the problem, replace the PDA.
11. Press the **Start** button.
12. Observe the **Authentication Code Request** screen.
13. Activate the keyboard screen on the PDA.
14. Enter the authentication code located on the PDA antenna.
15. Exit the keyboard screen.
16. Press **Enter** on the PDA screen.
17. Observe the busy icon on the PDA screen, then observe the Incident Information screen.
18. Press **Go** on the **Enter Incident Information** screen.
19. Observe a number of audible alerts corresponding to the number of active RSNs in the island of coverage, established in step 3 and the appearance of the Main screen on

the PDA. You may visually see the RSNs present by selecting the orange Pending tab on this screen.

20. Terminate the incident.
21. Cycle the power using the ignition switch. Wait for the LEDs on both the MMR and GS to be blinking mostly off with a short half-second on cycle.
22. Observe the equipment reboot and initiate another incident.
    The RSN will now present themselves on the PDA as unassigned resources. If this fails to produce the desired indication, detailed troubleshooting must be performed.

9.3 Hardware Troubleshooting

This following paragraphs provide an overview of a simple, but effective, method of troubleshooting. Use this seven-step process when you suspect an equipment failure:

- Gather information
- Understand the malfunction
- Identify which parameters need to be evaluated
- Identify the source of the problem
- Repair the equipment
- Verify the repair
- Perform a Cause Analysis

1. **Gather Information**
   Gathering information is a logical first step when troubleshooting equipment. Ask about or perform the following:
   - Gather all available technical documentation.
   - Make certain you understand how the equipment is intended to operate. In other words, that you have a detailed description of the symptom.
   - Review all equipment logs or other records that exist for the equipment.
   - Ask if any maintenance has been performed recently.
2. **Symptom Recognition**
   Symptom recognition means that you understand exactly how the equipment normally operates under these conditions and exactly what the equipment is doing at this time that is contrary to that normal operation. Make certain you have taken note of all indicators. Utilize all of your physical senses: hearing, sight, smell, etc. Take note of anything at all out of the ordinary. This is often considered the most important of all troubleshooting steps. If symptom recognition is not properly performed, you may proceed along an error-ridden line of logic, wasting time and experiencing excessive equipment downtime.

3. **Identify which parameters need to be evaluated.**
   Identifying which parameters need to be evaluated requires a clear understanding of the discrepancy and which signals affect the suspected component. Which input signals control the component? What is the expected output from the suspect circuit? Is there a timing delay, sequence, or set point that can be verified?

4. **Identify the source of the problem.**
   Identifying the source of the problem requires the technician to isolate components and evaluate circuit parameters; to isolate the circuit by group when dealing with a complicated circuit (half-step approach); and to identify the malfunctioning component using the recorded data.

5. **Correct/repair the component.**
   Correct or repair the component identified as damaged based on the recorded data. Perform the required repairs to the circuit. Completing step 5 can range from simple adjustments to a complete component replacement.

6. **Verify the repair.**
   Verify the repair after completion. Ensure the equipment is operating as designed. Perform another round of testing to verify the equipment is in fact running correctly and that no other discrepancies exist. Often this is referred to as performance of an operational checkout.

7. **Perform root cause analysis.**
   Performing a root cause analysis, even though mentioned last, began in the first step of the troubleshooting process. You should use the knowledge gained throughout the troubleshooting process in determining what could have possibly caused the component to fail.

   Did the component fail prematurely? Without identifying the possible cause that led to the failure, the repair will always be only temporary. While working through the troubleshooting process, ask yourself, “Is this the root cause or just a symptom of the problem?”

By following a well thought-out systematic process when challenged with an electrical troubleshooting problem, you will greatly enhance your effectiveness. Invest a little time up front doing your research and determining your troubleshooting plan of action.

System Troubleshooting Index

Click a link below to go directly to the steps to correct one of typical problem.

Gateway Router will not power up

Gateway Server will not power up

MMR System will not power up

System will not power up

Ethernet Switch will not power up

PDA will not run an incident

Multiple RSNs will not register on PDA during an incident

Gateway Router Will Not Power Up

Step	Yes *Go to step*	No *Go to step*
1. Disconnect the power connector at the base of the Gateway Router.	-	-
2. Using a Digital Volt Meter (DVM), check the DC Voltage level on the connector. Is it 12 VDC ±1.5 VDC? 3 4	3	4
3. Replace the Gateway Router.	End	End
4. Reconnect the connector disconnected in step 2 above.	-	-
5. Refer to the wiring diagram and determine the terminals on the distribution barrier strip that supply 12 VDC to the Gateway Router.	-	-
6. Using a DVM, check these terminals for 12 VDC. Is 12 VDC ±1.5 VDC present?	7	12
7. Disconnect the positive and negative wires that supply 12VDC to the Gateway Router from the distribution barrier strip.	-	-
8. Disconnect the power connector at the base of the Gateway Router.	-	-
9. Check the connector pins and associated wires for continuity. Is continuity present?	11	10
10. Repair or replace wiring as indicated.	End	End
11. Power connector on the Gateway Router is defective. Replace the Gateway Router.	End	End
12. Repair the terminal on the distribution barrier strip.	End	End

Gateway Server Will Not Power Up

Step	**Yes** *Go to step*	**No** *Go to step*
1. Disconnect the power connector that supplies a 12 VDC input to the Gateway Server.	-	-
2. Using a DVM, check the DC Voltage level on the connector. Is it 12 VDC ±1.5 VDC?	3	4
3. Replace the Gateway Server.	End	End
4. Reconnect the connector disconnected in step 2 above.	-	-
5. Refer to the wiring diagram and determine the terminals on the distribution barrier strip that supply 12 VDC to the Gateway Server.	-	-
6. Using a DVM, check these terminals for 12 VDC. Is 12 VDC ±1.5 VDC present?	7	12
7. Disconnect the positive and negative wires that supply 12VDC to the Gateway Server from the distribution barrier strip.	-	-
8. Disconnect the power connector at the base of the Gateway Server.	-	-
9. Check the connector pins and associated wires for continuity. Is continuity present?	11	10
10. Repair or replace wiring as indicated.	End	End
11. Power connector on the Gateway Server is defective. Replace the Gateway Server.	End	End
12. Repair the terminal on the distribution barrier strip.	End	End

MMR System Will Not Power Up

Step	Yes *Go to step*	No *Go to step*
1. Disconnect the power connector that supplies a 12 VDC input to the MMR System	-	-
2. Using a DVM, check the DC Voltage level on the connector. Is it 12 VDC ±1.5 VDC?	3	4
3. Replace the MMR System.	End	End
4. Reconnect the connector disconnected in step 2 above.	-	-
5. Refer to the wiring diagram, and determine the terminals on the distribution barrier strip that supply 12 VDC to the MMR System.	-	-
6. Using a DVM, check these terminals for 12 VDC. Is 12 VDC ±1.5 VDC present?	7	12
7. Disconnect the positive and negative wires that supply 12 VDC to the MMR System from the distribution barrier strip.	-	-
8. Disconnect the power connector at the base of the MMR System.	-	-
9. Check the connector pins and associated wires for continuity. Is continuity present?	11	10
10. Repair or replace wiring as indicated.	End	End
11. Power connector on the MMR System is defective. Replace the MMR System.	End	End
12. Repair the terminal on the distribution barrier strip.	End	End

System Will Not Power Up

Step	**Yes** ***Go to step***	**No** ***Go to step***
1. Using a DVM, check the DC Voltage level on the high current barrier strip. Is it 12 VDC ±1.5 VDC?	13	12
2. Verify that the high-current ON/OFF switch is in the ON position.	4	3
3. Place high-current ON/OFF switch is in the ON position.	-	-
4. Test the battery. Is it fully charged and operational?	6	5
5. Replace the battery.	End	End
6. Verify that the battery terminals are clean and that the connectors themselves are free of corrosion and properly torqued.	8	7
7. Disconnect battery, and disconnect positive and negative wire from high current barrier strip.	-	-
8. Using a DVM, check for continuity.	10	9
9. Repair or replace wiring as indicated.	End	End
10. Repair the Distribution Barrier Strip.	End	End

Ethernet Switch Will Not Power Up

Step	**Yes** ***Go to step***	**No** ***Go to step***
1. Refer to the power distribution diagram, and locate the output side of the distribution barrier strip and the two terminal studs that supply + and – 12VDC to the Ethernet switch.	-	-
2. Check for 12VDC ±1.5 at the terminal studs located above.	4	3
3. Repair connections on the distribution barrier strip.	End	End
4. Check for 12 VDC ±1.5 VDC at the input of the Ethernet switch. Is voltage present?	5	6
5. Replace the Ethernet switch	End	End
6. Repair or replace the wiring between the distribution barrier strip and the Ethernet switch.	End	End

PDA Will Not Run an Incident

Step	**Yes** ***Go to step***	**No** ***Go to step***
1. Did you have an opportunity to enter the authentication code?	2	7
2. Verify that all equipment is powered up. Are all components powered up?	3	6
3. Verify that the SSID is correct between the wireless access point and the PDA. Is the SSID correct?	4	5
4. Replace the PDA.	End	End
5. Correct the SSID.	End	End
6. Refer to the symptom list and troubleshoot the correct symptom.	End	End
7. Did the PDA power up?	8	4
8. Replace the battery in the PDA.	End	End

Multiple RSNs Will Not Register on PDA During an Incident

Step	Yes *Go to step*	No *Go to step*
1. Check that the Gateway Router is active by observing the activity indicator on the Ethernet switch at the port in which the Gateway Router is plugged. Is the Gateway Router active?	2	8
2. Wait for an appropriate period of time. This period of time could be as great as 10 minutes if a large number of RSNs have to enter the system.	-	-
3. As time passes, are more RSNs entering the network?	4	5
4. There is a variable delay between the beacon rate of the Gateway Router and the RSN that will result in this delay. As long as the backlog is clearing, this is likely a normal event.	End	End
5. Verify that the RSN(s) that will not enter the network have been properly configured in terms of area and class IDs. Is the configuration complete and correct?	6	7
6. Replace the RSN.	End	End
7. Properly configure the RSNs in question for the applicable area and class.	End	End
8. Is the Gateway Router powered up?	9	10
9. Replace the Gateway Router.	End	End
10. Refer to the symptom list and troubleshoot the correct symptom.	End	End

See also How to Wake Up or Troubleshoot an RSN.

10.0 Warranty, Technical Support, and Returning Equipment

10.1 Incident Management System (IMS) Warranty

The following is the THN warranty policy from our System Purchase Agreement. Unless the customer buys the equipment directly from a third-party supplier (such as PDAs purchased directly from Motorola), the warranty above will cover all equipment that TeraHop Networks ships. PDAs purchased directly from a third party are covered under that party's warranty.

1. Equipment -- Limited Warranty.

(a) Scope of Equipment Warranty. Subject to the limitations set forth herein, TeraHop warrants to Buyer that, during the Warranty Period (as defined below), the TeraHop equipment shall perform substantially in accordance with the technical specifications for such equipment in effect at Acceptance. The “Warranty Period” for each item of equipment shall be twelve (12) months from Acceptance (if applicable) or thirteen (13) months from initial Delivery of Equipment, whichever is shorter. This warranty does not cover (i) service calls, transportation charges, and non-emergency requests made outside normal business hours; (ii) routine checkouts and/or tuning; (iii) any equipment or part which is normally consumed in operation or has a normal life inherently shorter than the Warranty Period; (iv) alterations to standard equipment or Software requested by Buyer, or (v) any equipment part that is not properly stored, installed (unless installation is performed by TeraHop), used, or maintained, is repaired other than by TeraHop, is modified other than pursuant to TeraHop’s written approval, is harmed by any failure by Buyer properly to diagnose any problem, or has been subjected to any other kind of misuse, detrimental exposure, or damage, whether as the result of any accident or casualty. Upon TeraHop’s request, Buyer shall provide reasonable support to assist TeraHop in performing warranty services.

(b) TeraHop’s Warranty Obligations. If any equipment fails to meet the stated warranty, and provided that TeraHop performed or certified the installation, TeraHop will use reasonable efforts to correct the failure by, at its option, (i) repairing the defective or damaged component, (ii) replacing a defective component that has been returned, at the cost of Buyer, to TeraHop’s factory with a new or reconditioned component, or (iii) refunding to Buyer the purchase price of the component, pro rated to reflect the remaining warranty period. Any new or reconditioned part shall be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer. Standard delivery return shipments shall be paid for by TeraHop. Expedited handling, on-site visits, and all other services not covered by the above warranty shall be billed by TeraHop.

(c) EXCLUSIONS. ANY DEFECTS CAUSED BY ACTS OF GOD INCLUDING BUT NOT LIMITED TO LIGHTNING, EARTHQUAKES, FLOODS ETC. ARE NOT COVERED BY THE TERAHOP WARRANTY.

(d) Radio Frequency Network Coverage and Availability Disclaimer. Although care has been taken in designing the System to provide highly reliable radio frequency communications links between the various components, continuous, uninterrupted operation cannot be guaranteed. Radio waves are subject to blockage and attenuation by manmade and natural obstructions. Further, based upon movable or fixed structures, intermittent signal reflections may also adversely affect the ability to receive a signal from time to time. Finally, radio frequency noise from other users and/or accidental interference from improperly operating devices may also impact the ability to properly receive and decode signals. If persistent coverage issues that impact the overall System's operation are uncovered, TeraHop will work with Buyer to analyze the situation, identify the root cause, and recommend corrective action. Remedies may involve the need for Buyer to reposition or purchase some additional equipment. Costs associated with these changes will be the responsibility of Buyer.

(e) LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL TERAHOP OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, PUNITIVE OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, DAMAGES FOR LOSS OF GOOD¬WILL, COMPUTER FAILURE OR MALFUNCTION, OR ANY OTHER PECUNIARY LOSS) INCURRED BY BUYER OR ANY OTHER THIRD PARTY, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, INDEMNITY, WARRANTY, STRICT LIABILITY OR TORT AND REGARDLESS OF WHETHER TERAHOP OR ITS SUPPLIERS WERE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

(f) LIMITATION ON DAMAGES. IF TERAHOP BECOMES LIABLE TO BUYER FOR ANY MATTER ARISING OUT OF OR IN ANY WAY RELATING TO THIS AGREEMENT (INCLUDING THIS SECTION 9), WHETHER BASED ON AN ACTION OR CLAIM IN CONTRACT, TORT, OR OTHERWISE, THE AMOUNT OF DAMAGES RECOVERABLE AGAINST TERAHOP SHALL NOT EXCEED THE AGGREGATE AMOUNT PAID BY BUYER TO TERAHOP FOR THE SPECIFIC SERVICES, UNIT OF EQUIPMENT OR SOFTWARE GIVING RISE TO SUCH LIABILITY DURING THE ONE (1) YEAR PERIOD IMMEDIATELY PRECEDING BUYER'S CLAIM. BUYER ACCEPTS THE TERMS AND CONDITIONS OF THIS AGREEMENT WITH THE UNDERSTANDING THAT TERAHOP'S LIABILITY IS LIMITED, THE PRICES PAYABLE HAVE AND WILL BE CALCULATED ACCORDINGLY, AND THAT BUYER MAY REDUCE ITS RISK FURTHER BY MAKING APPROPRIATE PRO¬VISION FOR INSURANCE. BUYER AGREES TO MITIGATE ANY LOSSES OR DAMAGES.

(g) EXCLUSIVE REMEDIES. IT IS EXPRESSLY AGREED THAT, WITH THE EXCEPTION OF BUYER'S RETURN AND TERMINATION RIGHTS, THE STATED WARRANTIES CONSTITUTE TERAHOP'S SOLE OBLIGATION AND BUYER'S EXCLUSIVE REMEDIES FOR ANY CAUSE WHATSOEVER RELATING TO THIS AGREEMENT (INCLUDING, WITHOUT LIMITATION, ANY CAUSE RELATING TO A SOFTWARE AND DOCUMENTATION LICENSE), WHETHER BASED IN WARRANTY, CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, OR OTHERWISE, AND HOWEVER INSTITUTED, AND ALL OTHER REMEDIES OF ANY KIND ARE EXPRESSLY EXCLUDED AND DISCLAIMED. UPON EXPIRATION OF THE WARRANTY PERIOD, ALL SUCH LIABILITY SHALL TERMINATE. NO AGENT OR EMPLOYEE OF TERAHOP IS AUTHORIZED TO MAKE ANY MODIFICATION OR ADDITION TO THE STATED WARRANTY.

(h) No Other Warranties. THE WARRANTIES HEREIN ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED. To the maximum extent permitted by applicable law, TeraHop and its suppliers disclaim all other warranties and conditions, either express or implied, including, but not limited to, implied warranties of merchantability, fitness for a particular purpose, title, and non-infringement, with regard to any equipment, software and services provided under this Agreement. The only warranty provided with respect to Software is as set forth in the License Terms.

10.2 Incident Management System (IMS) Warranty Service and Technical Support

For technical service, in the U.S. contact TeraHop Networks using the information below.

Call TeraHop Customer Service at 770-663-3455.

Email TeraHop at Customer.Service@TeraHop.com.

Future: link to a page about the TeraHop Customer Management system (CMS), instructions how to login and how to use the system, documents you can download.

Future: tips, troubleshooting.

For information on how to obtain a return material authorization number, see How to Return Equipment.

10.3 How to Return Equipment

10.3.1 Return Material Authorization (RMA) Process Overview

The process is initiated by a TeraHop Networks (THN) Channel Partner (CP) or customer contacting THN Customer Service (CS) and requesting permission to return a component due to a defect. The TeraHop Networks Customer Service Technical Support Analyst (TSA), in conjunction with the requesting party, will determine the reason for the return request, assign an RMA number, and either email or point the requestor to the RMA form located on the online TeraHop Networks **Customer Relationship Management (CRM) System**. The CP or customer will specify if the repair/return option or swap/return option should be used, and mark the RMA form appropriately. Turnaround time for repair/return and swap/return parts will be according to the standard time frame shown in the table below. After the defective part is received, the timeframe for the turnaround of the repair/return or swap/return begins. Once you verify the replacement part is functioning properly, and the defect (if any) is documented by THN, THN CS will close the RMA.

When you (the CP) need an RMA number, do the following:

1. If you have the part in stock, replace the defective part within the system.
2. Call THN CS to request an RMA.
3. If the part is under warranty or a subsequent maintenance agreement, the THN TSA issues an RMA number to you.
4. If the part is not under warranty or a subsequent maintenance agreement, THN will notify you that you will be billed for the replacement part and labor. If you agree, the THN TSA issues an RMA number to you.
5. Specify on the RMA form if the repair/return option or swap/return option is to be used.
6. Return the part to THN along with the completed RMA form. The turnaround time is outlined in the table below.
7. THN follows the return option on the RMA form and sends back the repaired/swapped part.
8. THN bills for out of warranty (OOW) parts and labor. The costs are outlined in the table below.
9. Upon receipt, install the repaired/swapped part and confirm that it is working properly. The THN TSA will follow up with you (after notification from THN Manufacturing that the replacement part has been shipped) to verify the part is working properly. This follow-up will be either by phone call or e-mail, and will be required in order to close out the RMA process.
10. Once you confirm that the new part is received and/or working properly, THN closes the RMA.
11. THN will analyze the defective part and inform you of the findings.

Table 7: Maintenance Pricing Effective July 1, 2009

Maintenance Pricing Effective July 1, 2009			THN Turnaround Time (work days)
		Item $	
Remote Sensor Nodes			
Battery Replacement			
RSN-1	Field Battery Replacement Kit (Battery Pack, RSN Gasket, Instructions)	$18.00	
RSN-2	Factory Battery Replacement	$40.00	4
Case Replacement			
RSN-3	Factory Battery and Case Replacement	$50.00	4
Inoperable RSN (options are not compounded - pick only one)			
RSN-4	Diagnostic Analysis	$30.00	3
RSN-5	Diagnostics and s/w, firmware, and/or profile corrections	$60.00	4
RSN-6	Diagnostics and hardware repair	$120.00	10
RSN-7	Diagnostics and unit replacement (new UID)	$160.00	5
RSN-8	Annual RSN Factory Maintenance Agreement, per RSN (covers battery and case replacement when required, all hardware failures). Does not cover physical abuse.	$36.00	5
Mobile Gateway (MGW)			
MGW-1	Factory Housing Replacement (includes Housing, Batteries, Gaskets, factory default settings, and operational confirmation).	$225.00	5
MGW-2	Diagnostic Analysis	$210.00	4
MGW-3	Diagnostics and s/w, firmware, and/or configuration corrections	$250.00	5

MGW-4	Diagnostics and Gateway Router hardware repair (not to exceed...)	$350.00	10
MGW-5	Diagnostics and Gateway Router hardware replacement (one-for-one basis only)	$1,500.00	5
MGW-6	Diagnostics and IMX PC hardware replacement (one-for-one basis only)	$1,350.00	10
MGW-7	Diagnostics and IMX PC hardware repair (not to exceed...)	$475.00	15
MGW-8	Annual MGW Factory Maintenance Agreement, per MGW (covers Gateway Router and IMX Server replacement when required, all hardware failures). Does not cover physical abuse.	$1,500.00	
Third-Party Components (applies to **each** component returned)			
TPC-1	Diagnostic analysis and repair of PDA or Laptop	$100/hour + parts & shipping	TBD
TPC-2	Field PDA Extended Warranty, three years, channel partner coordinated	$275.00	
TPC-3	Field ADMS Server Extended In-Field Warranty, three years, channel partner coordinated	$150.00	
TPC-4	Factory PDA Extended Warranty, three years, THN coordinated	$425.00	30
TPC-5	Factory ADMS Server Extended In-Field Warranty, three years, THN coordinated.	$225.00	30
All Factory Options Include Return Shipping Charges			

11.0 Reference Information

11.1 Incident Management System (IMS) Warranty Service and Technical Support

For technical service, in the U.S. contact TeraHop Networks using the information below.

Call TeraHop Customer Service at 770-663-3455.

Email TeraHop at Customer.Service@TeraHop.com.

Future: link to a page about the TeraHop Customer Management system (CMS), instructions how to login and how to use the system, documents you can download.

Future: tips, troubleshooting.

For information on how to obtain a return material authorization number, see How to Return Equipment.

11.2 Appendix A: Vendor Data Sheets

Motorola Symbol MC70 Enterprise Digital Assistant (EDA) Rugged Handheld personal digital assistant (PDA). http://www.motorola.com/staticfiles/Business/Products/Mobile Computers/Handheld Computers/MC70/_Documents/Static Files/MC70_DS_1205.pdf

Garrett Magnum S14 4-port 10/100 MB Convenient Switch

http://www.lanstore.com/techsupport/hardware/datasheets/s14ds.pdf

11.3 Appendix B: Spare Parts Recommended List

TeraHop Networks recommends the following spares be kept in stock. Ideally, 1 unit spare should be kept in stock for every installed system.

Table 8: Spare Parts Recommended List

Part	Quantity to Keep in Stock
Gateway Router – GRXXXX-100-a-000-XXXXX	1 spare per every 5 units purchased
Application and MMR System – SRAPPX-100-a-000-XXXXX	1 spare per every 8 units purchased
Gateway Server – SRGWX-100-a-000-XXXXX	1 spare per every 8 units purchased
PDA – PDAXXX-100-a-000-XXXXX	1 spare per every 10 units purchased
PDA Stand Charger – CHPDAX-100-a-000-XXXXX	1 spare per every 20 units purchased
PDA Multi-Unit (4) Stand Charger – CHPDAX-101-a-000-XXXXX	1 spare per every 8 units purchased
PDA 12V Vehicle Lighter Charger – CHPDAX-102-a-000-XXXXX	1 spare per every 20 units purchased
Garrett Ethernet Switch – DC rated – ACETHX-100-a-000-XXXXX	1 spare per every 15 units purchased
RSN – RSNXXX-100-a-000-XXXXX	1 spare per every 10 units purchased
Mobile Installation Package – KMTGWM-100-a-000-XXXXX	1 spare per every 10 packages purchased

11.4 Appendix C: Tool Set

TeraHop Networks recommends that TeraHop Field Technicians have the following tool set for the installation of the Incident Management System.

- Equipment carrying case
- Socket wrench set
- Crescent wrench
- Hammer
- Crimping tool
- Wire cutters
- Torque head (T-20) for screwdriver
- Allen head for screwdriver (to fit 5/8 hex socket nylon screw on Gateway Router)
- Step-ladder – 6 foot foldable
- Flashlight
- Power strip
- Extension cord
- Two-sided Velcro tape
- Tube of silicon (if it becomes a recommendation to squirt inside the GR Ethernet port)
- Volt meter
- Bag of tie wraps
- RSN Configuration Tool (software, when available)

11.5 Appendix D: Incident Management System with Automated Accountability System Component Specifications

The TeraHop Incident Management System (IMS) *with* Automated Accountability that is supplied by TeraHop Networks includes several hardware and software components. The quantity of each component that is required for a given customer depends on the customer’s organizational structure, size, ratios of people to vehicles and equipment, etc.

This section describes the major specifications for each of the system components. The diagram below shows the major components of the TeraHop IMS solution.

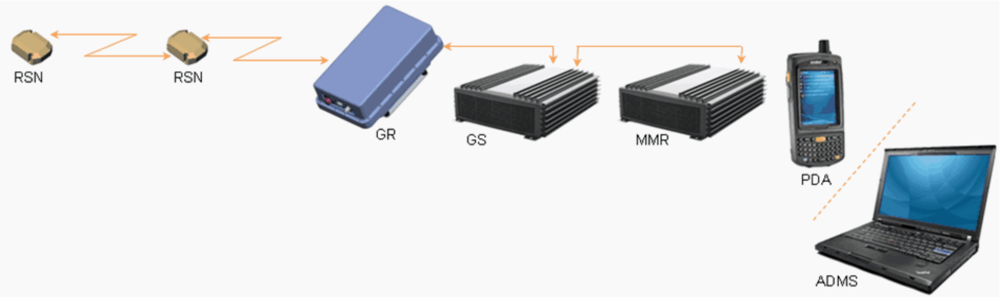


Figure 23: End-to-End System Components

RSN – Remote Sensor Node

GR – Gateway Router

GS – Gateway Server

GC – Gateway Controller – combination of GR and GS (not shown)

MMR – Message Management and Routing System computer

PDA – Personal Digital Assistant

ADMS – Administration System

11.5.1 Remote Sensor Node (RSN)

Hardware

Dimensions:	2.4” x 3.6” x 1.2” (6.1 cm x 9.0 cm x 2.9 cm), nominal
Weight:	6 ounces, including internal batteries (170 g)
Power (internal):	Two (2) type A Lithium, 3V, 3.0 AH (non-user-replaceable)
Power Requirements:	No external required
Color:	Industrial grey
Expansion Port:	One (1) 16-pin for GPIO and serial connections
Transceiver 1:	Proprietary low-power packet radio (wake-up radio)
Transceiver 2:	Class 1 Bluetooth®
Frequency Band:	2.4 GHz, unlicensed (globally)
Antennas:	Internal
Housing Material:	ABS

Software/Firmware

Operating System:	TeraHop Operating System
Other:	TeraHop Networks RSN Firmware
Environmental Performance	
Operating Temperature Range:	-25°C to +55°C (-77°F to +131°F)
Humidity:	100%, condensing
Shock:	Four (4)-foot drop on concrete without damage
Immersion:	30 min. in water of 1m. head, per IP-67
Vibration:	30g, 6-axis
Salt fog:	ASTM B 117-07 (21 days)
Regulatory Compliance	
	FCC Part 15C, Class B

Bluetooth is a registered trademark of Bluetooth SIG, Inc.

11.5.2 Gateway Router

Hardware	
Dimensions:	13.8” x 8” x 5” (35 cm x 20.3 cm x 12.7 cm), nominal
Weight:	12lbs. (5.4 kg)
Power Requirements:	12VDC @ 1.5A
Color:	Industrial grey
Transceiver 1:	Proprietary low-power packet radio (wake-up radio)
Transceiver 2:	Class 1 Bluetooth
GPS:	GPS receiver with data reporting
Wi-Fi Transceivers:	802.11a, two each
Ports:	• Power, keyed, circular, w/cover, sealed • 10/100 Ethernet RJ-45, w/ cover, sealed • Serial data, 9-pin, circular, w/cover, sealed
Antennas:	Internal
Housing Material:	ABS
Other:	Real Time Clock
UPS, internal	
Optional Radios:	GSM, CDMA
Environmental Performance	
Operating Temperature Range:	-25°C to +55°C (-13°F to +131°F)
Shock:	Four (4)-foot drop on concrete without damage
Immersion:	30 min. in water of 1m. head, per IP-67
Vibration:	20g, 6-axis
Salt fog:	ASTM B 117-07 (21 days)
Software	
Operating Systems:	Linux OS TeraHop Operating System
Other:	TeraHop Networks GR Application
Regulatory Compliance	
	FCC Part 15C, Class B

11.5.3 Gateway Server (Non-Integrated)

Hardware	
Dimensions:	8.3” W x 10” L x 2.2” H (21 cm x 25 cm x 56 cm)
Weight:	7 lb (3.17 kg)
Power Requirements:	12VDC @ 4 Amps
Processor:	Intel Core 2 Duo Processor 2.0GHz
RAM:	3GB
Storage:	80GB Hard Drive
Ports:	Power 10/100 Ethernet RJ-45
Cooling:	Twin 5CFM ultra-quiet fans
Environmental Performance	
Operating Temperature Range:	-20°C to +70°C (-4° to +158°F)
Humidity:	100%, non-Condensing
Software	
Operating System:	Linux Fedora 10
Other:	TeraHop Networks GS Software

11.5.4 Management and Routing (MMR) Server

Hardware

Dimensions:	8.3” W x 10” L x 2.2” H (21 cm x 25 cm x 56 cm)
Weight:	7 lb (3.17 kg)
Power Requirements:	12VDC @ 4 Amps
Processor:	Intel Core 2 Duo Processor, 2.0GHz
RAM:	3GB
Storage:	80GB hard drive
Ports:	Power 10/100 Ethernet RJ-45
Cooling:	Twin 5CFM ultra-quiet fans

Environmental Performance

Operating Temperature Range:	-20°C to +70°C (-4° to +158°F)
Humidity:	100%, non-Condensing

Software

Operating System:	Microsoft Windows Server 2003
Other:	TeraHop Networks MMR Software

11.6 TeraHop Networks IMS Application

Administration Station (ADMS) Laptop Computer

Hardware

Type/Brand:	Lenovo ThinkPad SL500 Series laptop computer
Processor:	Intel Core 2 Duo
Display:	15.4-inch WXGA, antiglare
Wi-Fi:	802.11a/g/n
RAM:	3GB
Storage:	250GB Hard Drive

Software

Operating System:	Microsoft Windows XP Professional
Other:	

TeraHop Console (THC)

Optional Plug-Ins:	• Incident Log Extraction Tool • RSN Configuration Tool (RCT) • ADMS-MMR Data Services • Mobile Gateway Configuration Tool • IMS Application Configuration Tool

Personal Digital Assistant (PDA)

Hardware

Model/Type:	Motorola (Symbol) MC7094
Dimensions:	6” L x 3” W x 1.5” H (15.3cm x 7.6cm x 3.7cm)
Display:	Touch-screen, color 3.5” QVGA
Keyboards:	• Physical QWERTY keyboard • Virtual (OS-based)
Scanner:	2D laser scanner (barcode)
Modem:	Integrated GSM EDGE cellular modem
Transceiver:	Bluetooth
Wi-Fi:	802.11a/g/n
Memory Expansion:	SD memory card slot
Battery:	3.7V, 3800 mAH extended capacity
Included Accessories:	Single-slot charging/interface cradle kit (110VAC input)
Optional Accessories:	• 12VDC cigarette-lighter vehicle charger • Vehicular charging cradle (12VDC input) • 4- slot charging cradle (110VAC input)

TeraHop Networks IMS PDA Application (continued)

Software

Operating System:	Windows Mobile 5.0
Other:	TeraHop IMS Client Application

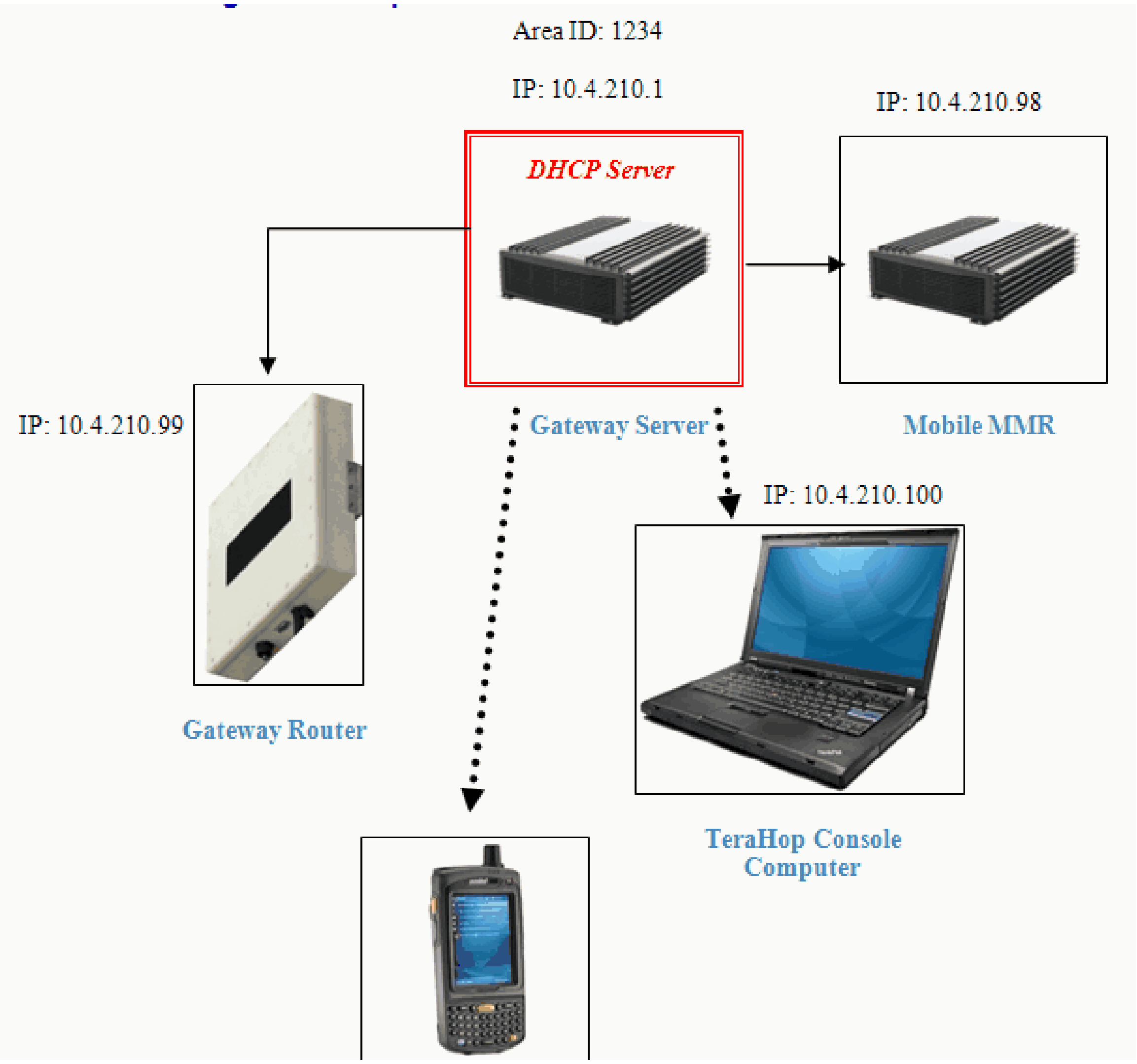
11.7 Appendix E: Description of Mobile Gateway System Ethernet Connectivity

11.7.1 IP Address Assignment Methodology

The Mobile Gateway System uses DHCP as a method of distributing an IP address for each of the individual components in the system. The Gateway Server acts as the DHCP Server. The Gateway Router, Mobile-MMR, PDA Clients, and the TeraHop Console Computer all act as DHCP Clients. No configuration is required to set IP address for any of the Mobile Gateway System Components. Configuration of Access Point SSID, however, is necessary for wirelessly connected components.

Each Gateway Server is assigned an Area ID by TeraHop Networks. This Area ID is unique to each Gateway Server and may not be changed. The Area ID provides the basis for all IP addresses and SSID in the Mobile Gateways System. IP address follow the following format: 10.A1.A2.x where A1 is the upper byte of the Area ID, A2 is the lower byte of the Area ID, and x is the unique integer assigned by the DHCP server to each component. For Example, if the Gateway Servers Area ID is 5 the IP Address of the system would be 10.0.5.x. If the Gateway Servers Area ID is 1234 the IP Addresses of the system would be 10.4.210.x.

IP Address Assignment Example



11.7.2 Calculating the IP Address Scheme

To calculate the middle two octets of the IP address, convert Area ID take the upper byte (A1), in decimal as the second octet and the lower byte (A2), in decimal, as the third octet.

	Hex	Dec
Area ID	0x04D2	1234
A1	0x04	4
A2	0xD2	210

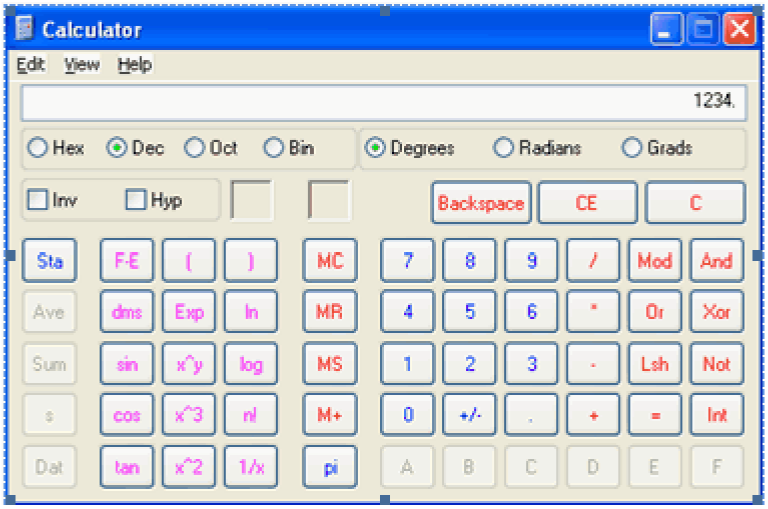
The resulting IP Address is 10.4.210.x

11.7.2.1 Calculating the IP Address Scheme – Step By Step

To calculate the middle two octets of the IP Address from the Area ID do the following:

1. Open the Windows Calculator
   a. **Start -> Run**
   b. Type **calc**.
   c. Press **Enter**.
   d. From the **View** menu, select **Scientific**.

   The **Calculator** opens.


Calculator
Edit View Help
1234.
○ Hex ● Dec ○ Oct ○ Bin
● Degrees ○ Radians ○ Grads
□ Inv □ Hyp
Backspace CE C
Sta F-E ( ) MC 7 8 9 / Mod And
Ave dms Exp ln MR 4 5 6 * Or Xor
Sum sin x^y log MS 1 2 3 - Lsh Not
s cos x^3 n! M+ 0 +/- . + = Int
Dat tan x^2 1/x pi A B C D E F

2. Select the **Dec** radio button
3. Enter the Area ID (example: 1234)
4. Select the **Hex** radio button (example: 04D2).

5. Take the first two digits of the **Hex** value (example: 04), reenter them, and convert back to decimal by pressing the **Dec** radio button (example: 4). The result is A1.
6. Press the **C** button to clear
7. Select the **Hex** radio button, then reenter the second two digits of the **Hex Area ID** (example: D2)
8. Select the **Dec** radio button to convert them back to decimal (example: 210). This result is A2.
9. Combine the results of step 5 (A1) and step 8 (A2) into an IP Address 10.A1.A2.x (example: 10.4.210.x)

The Gateway Server always uses an IP Address with the fourth octet of 1, meaning the Gateway Severs IP Address with an Area ID of 5 would be 10.0.5.1. With an Area ID 1234 the Gateway Server's IP Address would be 10.4.210.1.

Both the Area ID and IP Address are listed on the label on the back of the gateway server.

11.7.2.2 Calculating Your IP Address Scheme

	Hex	Dec
My Area ID		
A1		
A2		

The resulting IP Address is:

11.7.2.3 Connecting TeraHop Console Computer to the Internet

The TeraHop Console Computer requires a connection to the Internet. This connection must be a wired connection via CAT5e cable or similar.

TeraHop Console Computer shall be located:

12.0 Glossary

C

CAUTION: Refers to a situation in which equipment may be damaged if the CAUTION is not observed.

D

Danger: Refers to a situation hazardous to personnel if the information in the DANGER is not observed. Likely consequences are severe injury or death.

DOA: Dead on Arrival

DVA: Digital Volt Meter

E

ESD: Electrostatic Discharge

ESS: Emergency Services Sector

F

FTP: File Transfer Protocol

G

GC: Gateway Controller. A GC contains a Gateway Server and a Gateway Router.

GR: Gateway Router

I

IC: Incident Commander

IMS: Incident Management System with Automated Accountability

M

MA: Maintenance Agreement

MMR: Message Management and Routing System

N

Note: Highlights critical information about a procedure or description. A Note does not describe hazards to personnel, equipment, or service.

O

OEM: Original Equipment Manufacturer

OOW: Out of Warranty

P

PDA: Personal Digital Assistant

POE: Power Over Ethernet

R

RMA: Return Material Authorization

RSN: Remote Sensor Node

T

THN: TeraHop Networks, Inc.

TSA: Technical Support Analyst

W

WA: Warranty

Warning: Refers to a situation hazardous to personnel if the information in the WARNING is not observed. Possible consequences are severe injury or death.

13.0 Index