System Release 2.8
MOTOTRBO™ Connect Plus

XRC Controller User Guide

JUNE 2017

68012002055–JC

Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

Furthermore, the purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a specific system, or may be dependent upon the characteristics of a specific mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

European Union (EU) Waste of Electrical and Electronic Equipment (WEEE) directive

The European Union's WEEE directive requires that products sold into EU countries must have the crossed out trash bin label on the product (or the package in some cases).

As defined by the WEEE directive, this cross-out trash bin label means that customers and end-users in EU countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

This page intentionally left blank.

Contact Us

Motorola Solutions Support Center

The Solutions Support Center (SSC) is the primary Motorola Solutions support contact. Call:

- Before any software reload.
- To confirm troubleshooting results and analysis before removing and replacing a Field Replaceable Unit (FRU) and Field Replaceable Entity (FRE) to repair the system.

For...	Phone
United States Calls	**800-221-7144**
International Calls	**302-444-9800**

North America Parts Organization

For assistance in ordering replacement parts or identifying a part number, contact the Motorola Solutions Parts organization. Your first response when troubleshooting your system is to call the Motorola SSC.

For...	Phone
Phone Orders	**800-422-4210** (US and Canada Orders) For help identifying an item or part number, select choice 3 from the menu.
	302-444-9842 (International Orders) Includes help for identifying an item or part number and for translation as needed.
Fax Orders	**800-622-6210** (US and Canada Orders)

Comments

Send questions and comments regarding user documentation to documentation@motorolasolutions.com.

Provide the following information when reporting a documentation error:

- The document title and part number
- The page number with the error
- A description of the error

We welcome your feedback on this and other Motorola Solutions manuals. To take a short, confidential survey on Motorola Solutions Customer Documentation, go to docsurvey.motorolasolutions.com or scan the following QR code with your mobile device to access the survey.

This page intentionally left blank.

Declaration of Conformity

This declaration is applicable to your radio only if your radio is labeled with the FCC logo shown below.

Declaration of Conformity

Responsible Party

Name: Motorola Solutions, Inc.

Address: 1303 East Algonquin Road, Schaumburg, IL 60196-1078, U.S.A.

Phone Number: 1-800-927-2744

Hereby declares that the product:

Model Name: **XRT 9000 / XRT 9100**

conforms to the following regulations:

FCC Part 15, subpart A

Class B Digital Device
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 in a residential area, the user is required to correct the interference at his own expense.

NOTICE: The user is cautioned that changes or modifications not expressly approved by Motorola could result in the equipment being noncompliant with FCC Class A requirements and void the user's authority to operate the equipment.

This page intentionally left blank.

Document History

Version	Description	Date
68012002055–JC	Original release of the *XRC Controller User Guide* for MOTOTRBO™ Connect Plus	June 2017

This page intentionally left blank.

Contents

This page intentionally left blank.

List of Figures

List of Procedures

Commercial Warranty

Limited Warranty

MOTOROLA COMMUNICATION PRODUCTS

What This Warranty Covers and For How Long

MOTOROLA SOLUTIONS INC. (“MOTOROLA”) warrants the MOTOROLA manufactured Communication Products listed below (“Product”) against defects in material and workmanship under normal use and service for a period of time from the date of purchase as scheduled below:

XRC 9000 Controller	Two (2) Years
XRC 9100 Controller	Two (2) Years

Motorola, at its option, will at no charge either repair the Product (with new or reconditioned parts), replace it (with a new or reconditioned Product), or refund the purchase price of the Product during the warranty period provided it is returned in accordance with the terms of this warranty. Replaced parts or boards are warranted for the balance of the original applicable warranty period. All replaced parts of Product shall become the property of MOTOROLA.

This express limited warranty is extended by MOTOROLA to the original end user purchaser only and is not assignable or transferable to any other party. This is the complete warranty for the Product manufactured by MOTOROLA. MOTOROLA assumes no obligations or liability for additions or modifications to this warranty unless made in writing and signed by an officer of MOTOROLA. Unless made in a separate agreement between MOTOROLA and the original end user purchaser, MOTOROLA does not warrant the installation, maintenance or service of the Product.

MOTOROLA cannot be responsible in any way for any ancillary equipment not furnished by MOTOROLA which is attached to or used in connection with the Product, or for operation of the Product with any ancillary equipment, and all such equipment is expressly excluded from this warranty. Because each system which may use the Product is unique, MOTOROLA disclaims liability for range, coverage, or operation of the system as a whole under this warranty.

General Provisions

This warranty sets forth the full extent of responsibilities of Motorola regarding the Product. Repair, replacement or refund of the purchase price, at the option of Motorola, is the exclusive remedy. THIS WARRANTY IS GIVEN IN LIEU OF ALL OTHER EXPRESS WARRANTIES. IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE LIMITED TO THE DURATION OF THIS LIMITED WARRANTY. IN NO EVENT SHALL MOTOROLA BE LIABLE FOR DAMAGES IN EXCESS OF THE PURCHASE PRICE OF THE PRODUCT, FOR ANY LOSS OF USE, LOSS OF TIME, INCONVENIENCE, COMMERCIAL LOSS, LOST PROFITS OR SAVINGS OR OTHER INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE SUCH PRODUCT, TO THE FULL EXTENT SUCH MAY BE DISCLAIMED BY LAW.

State Law Rights

SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES OR LIMITATION ON HOW LONG AN IMPLIED WARRANTY LASTS, SO THE ABOVE LIMITATION OR EXCLUSIONS MAY NOT APPLY.

This warranty gives specific legal rights, and there may be other rights which may vary from state to state.

How to Get Warranty Service

You must provide proof of purchase (bearing the date of purchase and Product item serial number) in order to receive warranty service and, also, deliver or send the Product item, transportation and insurance prepaid, to an authorized warranty service location. Warranty service will be provided by Motorola through one of its authorized warranty service locations. If you first contact the company which sold you the Product, it can facilitate your obtaining warranty service. You can also call Motorola at 1-888-567-7347 US/Canada.

What This Warranty Does Not Cover

1. Defects or damage resulting from use of the Product in other than its normal and customary manner.
2. Defects or damage from misuse, accident, water, or neglect.
3. Defects or damage from improper testing, operation, maintenance, installation, alteration, modification, or adjustment.
4. Breakage or damage to antennas unless caused directly by defects in material workmanship.
5. A Product subjected to unauthorized Product modifications, disassemblies or repairs (including, without limitation, the addition to the Product of non-Motorola supplied equipment) which adversely affect performance of the Product or interfere with Motorola's normal warranty inspection and testing of the Product to verify any warranty claim.
6. Product which has had the serial number removed or made illegible.
7. Rechargeable batteries if:
   - any of the seals on the battery enclosure of cells are broken or show evidence of tampering.
   - the damage or defect is caused by charging or using the battery in equipment or service other than the Product for which it is specified.
8. Freight costs to the repair depot.
9. Product, does not function in accordance with MOTOROLA’s published specifications or the FCC type acceptance labeling in effect for the Product at the time the Product was initially distributed from MOTOROLA.
10. Scratches or other cosmetic damage to Product surfaces that does not affect the operation of the Product.
11. Normal and customary wear and tear.

Patent and Software Provisions

MOTOROLA will defend, at its own expense, any suit brought against the end user purchaser to the extent that it is based on a claim that the Product or parts infringe a United States patent, and MOTOROLA will pay those costs and damages finally awarded against the end user purchaser in any such suit which are attributable to any such claim, but such defense and payments are conditioned on the following:

1. that MOTOROLA will be notified promptly in writing by such purchaser of any notice of such claim;
2. that MOTOROLA will have sole control of the defense of such suit and all negotiations for its settlement or compromise; and
3. should the Product or parts become, or in MOTOROLA's opinion be likely to become, the subject of a claim of infringement of a United States patent, that such purchaser will permit MOTOROLA, at its

option and expense, either to procure for such purchaser the right to continue using the Product or parts or to replace or modify the same so that it becomes noninfringing or to grant such purchaser a credit for the Product or parts as depreciated and accept its return. The depreciation will be an equal amount per year over the lifetime of the Product or parts as established by MOTOROLA.

MOTOROLA will have no liability with respect to any claim of patent infringement which is based upon the combination of the Product or parts furnished hereunder with software, apparatus or devices not furnished by MOTOROLA, nor will MOTOROLA have any liability for the use of ancillary equipment or software not furnished by MOTOROLA which is attached to or used in connection with the Product. The foregoing states the entire liability of MOTOROLA with respect to infringement of patents by the Product or any parts thereof.

Laws in the United States and other countries preserve for MOTOROLA certain exclusive rights for copyrighted MOTOROLA software such as the exclusive rights to reproduce in copies and distribute copies of such Motorola software. MOTOROLA software may be used in only the Product in which the software was originally embodied and such software in such Product may not be replaced, copied, distributed, modified in any way, or used to produce any derivative thereof. No other use including, without limitation, alteration, modification, reproduction, distribution, or reverse engineering of such MOTOROLA software or exercise of rights in such MOTOROLA software is permitted. No license is granted by implication, estoppel or otherwise under MOTOROLA patent rights or copyrights.

Governing Law

This Warranty is governed by the laws of the State of Illinois, USA.

Computer Software Copyrights

Open Source Software Legal Notices

This Motorola Product contains Open Source Software. For information regarding licenses, acknowledgments, required copyright notices, and other usage terms, refer to the Documentation for this Motorola Product at:

https://businessonline.motorolasolutions.com/

Go to:

Motorola Online>Resource Center>Product Information>Manuals>MOTOTRBO>Connect Plus

This page intentionally left blank.

About the XRC Controller User Guide

This User Guide provides installation and operation instructions for the MOTOTRBO™ Connect Plus XRC Controller.

What Is Covered in This Guide

The *XRC Controller User Guide*contains the following chapters:

- Introduction on page 31
- Safety Information on page 33
- Installation on page 35
- Communicating with the Device on page 61
- Site and Network Configuration on page 79
- System Management on page 113

In addition, this guide contains Appendix A Determining the UPS Capacity on page 187.

Helpful Background Information

Motorola Solutions offers various courses designed to assist in learning about the system. For information, go to http://www.motorolasolutions.com/training to view the current course offerings and technology paths.

Related Information

Related Information	Purpose
Standards and Guidelines for Communication Sites (6881089E50)	Provides standards and guidelines that should be followed when setting up a Motorola Solutions communications site. Also known as R56 manual.

This page intentionally left blank.

Chapter 1

Introduction

The XRC is a powerful multiprocessor computer designed to provide call processing and real-time resource management. It is designed as an Ethernet Internet Protocol (IP) device that can be configured for MOTOTRBO Connect Plus single site or multisite trunking operation. The XRC can support up to twenty-nine (29) voice/data channels per site and up to two hundred and fifty (250) RF sites when ordered for multi-site operation. The XRC 9000 is the original controller hardware platform. The XRC 9100 provides the same features as the XRC 9000, along with faster processing, more memory, and external heat dissipation.

There are more similarities than differences between the XRC 9000 and XRC 9100. Wherever a statement or feature description applies to both hardware platforms, the term "XRC" is used.

MOTOTRBO Connect Plus is the next generation professional digital trunking communications solution that provides more performance, productivity and value for your business. MOTOTRBO Connect Plus uses 2:1 Time Division Multiple Access (TDMA) technology with a control channel slot based architecture which provides the following key trunking features:

- PTT-ID
- Radio ID, Group ID, and ESN Validation
- Group Call, Multigroup Call, and Site All Call
- Network Wide All Call initiated by an XRT Client
- Emergency Call
- Emergency Alert
- Private Call/ Call Alert
- Dynamic Site Assignment
- Site Registration
- Site Restriction (network roaming privileges, configurable per Connect Plus subscriber)
- Automatic Roaming
- User Priority Levels
- Busy Queuing
- Remote Monitor
- Radio Check
- Text Messaging Capability with "Store and Forward"
- GPS updates for Automatic Vehicle Location (AVL) – with additional 3rd party software applications
- Over-the-air update capability for site/network frequency information, Connect Plus Option Board Codeplug, and Connect Plus Option Board Firmware files
- Centralized Network and Fault Management
- Redundant Trunking Controller (free option upon purchasing second XRC per site)
- Control Channel Rollover and Failover
- Repeater Call Hang Times configured with the Connect Plus Network Manager
- Auto Fallback
- Remote Repeater Programming

- Packet Data Call
- Telephone Interconnect Capable (requires the XRI Interconnect Gateway and other additional hardware)
- Priority Monitor Scan
- Fast GPS to enhance speed and throughput of periodic location updates.
- Generic Data Call
- Indoor Location Tracking for supporting subscriber radios. Requires additional third party software application.
- Talk Group Restriction by site
- Permanent Talk Group Registration by site
- Digital Base Station Identification (BSI) for supporting repeaters. Analog BSI when Digital BSI is not supported.

NOTICE: Refer to the *MOTOTRBO Connect Plus System Planner* for more details on system configurations and trunking features.

Chapter 2

Safety Information

For your protection, this product has been tested to various national and international regulations and standards. The scope of this regulatory testing includes electrical and mechanical safety, radio frequency interference, acoustics, and known hazardous materials. Where applicable, approvals obtained from the third-party test agencies are shown on the product label.

2.1 Grounding

This is a safety class I product and has protective grounding terminals. There must be an uninterruptible safety earth ground from the main power source to the product's input wiring terminals, power cord, or supplied power cord set.

IMPORTANT: Whenever it is likely that the protection has been impaired, disconnect the power cord until the ground has been restored.

If your LAN covers an area served by more than one power distribution system, ensure that their safety grounds are securely interconnected.

⚠ **CAUTION:** LAN cables may occasionally be subject to hazardous transient voltages such as lightning or disturbances in the electrical utilities power grid. Handle exposed metal components of the network with caution.

2.1.1 Network Connected Equipment

The installation must provide a ground connection for the network equipment.

2.1.2 Cable Connections

All Ethernet and serial ports are designed for connecting to equipment that is located in the same building as the device. Do **not** connect these ports directly to wiring that exits the building where the device is located.

2.2 Servicing

There are no user-serviceable parts inside this product. Any servicing, adjustment, maintenance, or repair must be performed only by a service-trained personnel.

This product has a power switch that must be used to power on the unit after the power cord is plugged in.

2.2.1 Lithium Battery Warning

The Lithium Battery used in device may not be replaced by the user. The Lithium Battery must be replaced by authorized service personnel with the same or equivalent type.

This page intentionally left blank.

Chapter 3

Installation

WARNING: This equipment must be provided with a proper AC protective earth (PE) ground connection.

3.1

Unpacking and Checking Equipment

The device comes wrapped in a plastic bag and secured in Styrofoam protective packaging.

Procedure:

1. Unpack all the individual parts.

   The packaging comes with the following list of items:

   - The device.
   - Power cable terminating in 120 Volt, male, three-prong connector, if specified in order.
   - Ethernet Crossover Cable.
   - Quick Start Guide CD.
   - Mounting kit:
     - Two (2) Handles with screws.
     - Two (2) Rack mounting brackets.
     - One (1) Bag of 12 Rack mounting screws.
2. Inspect the unit for any shipping damage.

   If you discover any damages, contact Motorola Solutions immediately. Keep the original packing material in case you need to ship the equipment.

3.2

Initial Power Up

3.2.1

Power Requirements

Input Voltage	100 to 240 VAC auto-ranging (47 to 63 Hz for AC power)
Power Consumption	9100 Model: 40 Watts

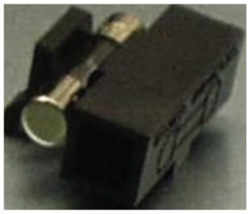
3.2.2

Fuse

The fuse is located underneath the AC Power Input connector (located on the right side of the rear panel).

The fuse can be replaced by using a small flat-head screwdriver to remove the fuse holder.

Figure 1: Fuse



3.2.3
Connecting the Power Cable

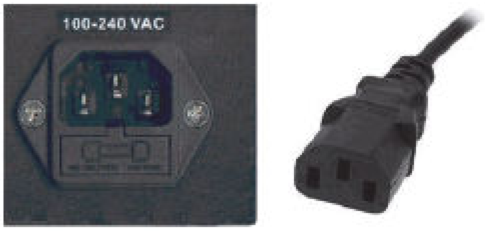
When and where to use:

IMPORTANT: Power should not be applied until all cables are attached and the unit is ready to operate.

Procedure:

1. Attach the cable-mounted female connector of the power cord to the panel-mounted male connector (inlet) of the device.
2. Attach the male end of the power cord to a properly grounded 100/240 VAC, 50/60 Hz outlet, UPS, power strip, or wall socket.

   Figure 2: Power Input Connector

3.2.4
On/Off Switch

The device activates once it has power applied through the power cord.

A short press of the On/Off switch powers the device up or down. Powering down by this method can take up to 30 seconds.

A long press of the On/Off switch powers down the device immediately. However, this method should be avoided, if at all possible (see the following caution).

NOTICE: If the device is powered down with the On/Off switch and then, the power is removed from the unit (unplugging the cord, power failure, etc), the device automatically powers up when power is restored to the unit.

CAUTION: Immediate shutdown (long press of the On/Off switch) can result in loss and/or corruption of data. This method should only be used if the normal power-down is unsuccessful. Any sudden loss of power (such as removing the power cord) can result in loss and/or corruption of data. This is why it is critical to utilize a UPS with the device.

3.3
Getting Acquainted with the 9100 Model

The sections which follow introduce the front panel and rear panel of the 9100 model device.

3.3.1 Front Panel

This section explains the indicators and ports found in the front panel of the device.

3.3.1.1 Front Panel Photo

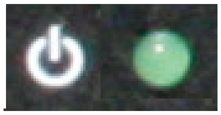
The following image shows the Front Panel of the 9100 model.

3.3.1.2 Indicators

3.3.1.2.1 Power LED

On the front panel of the device is a green LED marked with the POWER symbol. The LED illuminates when power is properly supplied to the unit and the POWER switch it turned to the on position.

Figure 3: Power LED

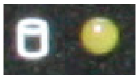


3.3.1.2.2 Storage Activity LED

The yellow LED, located on the right side of the front panel and below the Power LED.

The yellow LED indicates the storage (Hard Drive) activity. The yellow LED lights up when the Hard Drive is being accessed.

Figure 4: Storage Activity LED



3.3.1.2.3 PWR1 and PWR2 LEDs

PWR1 and PWR2 are red LEDs that are not currently used.

They are located to the immediate right of the Power and Storage Activity LEDs.

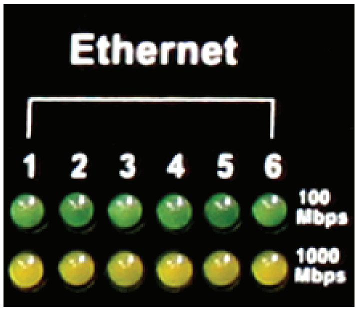
3.3.1.2.4 Ethernet Activity LEDs

The six pairs of Ethernet LEDs are labeled 1-6.

The number above the LED corresponds to the Ethernet port number (LAN1 through LAN6) on the rear panel of the device. For each Ethernet port, there is a green LED and a yellow LED. The LED illuminates continuously when carrier is present but no messages are being passed. The LED blinks when messages are present.

- The green LED lights up if the corresponding Ethernet port has activity at a 100 Mbps communications rate.
- The yellow LED lights up if the corresponding Ethernet port has activity at a 1000 Mbps communications rate.

Figure 5: Ethernet Activity LEDs



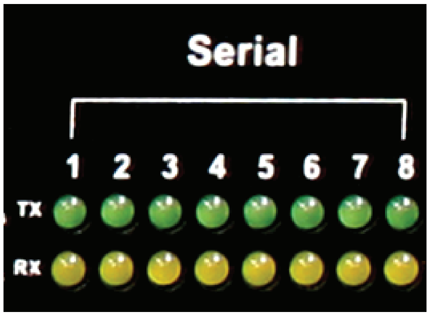
3.3.1.2.5 Serial Activity LEDs

The eight pairs of Serial LEDs are labeled 1-8.

The number above the LED corresponds to the serial port number (P1 through P8) on the rear panel of the device. For each Serial port, there is a green LED and a yellow LED.

- The green LED lights up for transmit (TX) activity on the corresponding serial port.
- The yellow LED lights up for receive (RX) activity on the corresponding serial port

Figure 6: Serial Activity LEDs



3.3.1.2.6 Programmable LEDs

The eight LEDs located in the area labeled “Programmable LED” are not currently used.

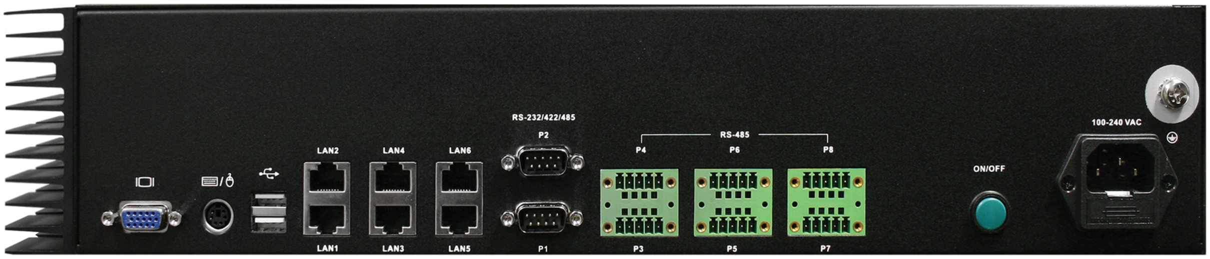
3.3.2 Rear Panel

This section explains the ports found in the rear panel of the device.

3.3.2.1 Rear Panel Photo

The following image shows the rear panel of the 9100 model.

Figure 7: XRC 9100 Rear Panel

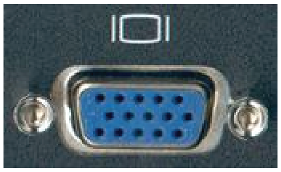


3.3.2.2 Ports

3.3.2.2.1 Video (VGA) Port

The VGA port is located on the left side of the rear panel. It can be used to attach a display monitor to the unit.

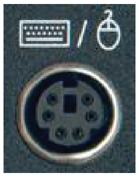
Figure 8: Video (VGA) Port



3.3.2.2.2 PS/2 Port

The PS/2 port is located on the left side of the rear panel and to the right of the VGA port. It is used for connecting a keyboard or a mouse.

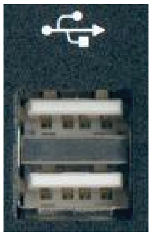
Figure 9: PS/2 Port



3.3.2.2.3 Universal Serial Bus (USB)

There are two USB ports located on the left side of the rear panel. The USB port is used for memory expansion, where applicable.

Figure 10: Universal Serial Bus (USB)

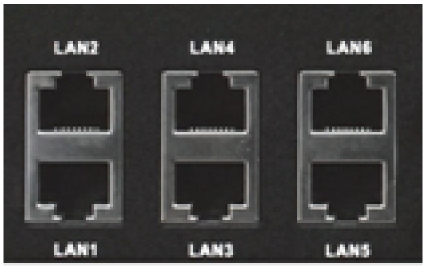


3.3.2.2.4

Ethernet Ports (6)

The six (6) Gigabit Ethernet LAN ports (labeled LAN1 to LAN6) are located on the rear panel and to the right of the USB ports.

Figure 11: Ethernet Ports



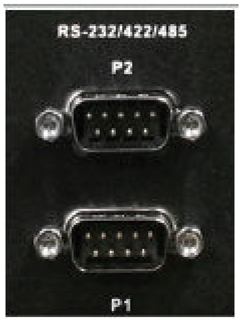
3.3.2.2.5

RS-232/422/485 Serial Ports (P1-P2)

The two (2) RS-232/422/485 Serial (COM) Ports are labeled P1 and P2. They are located on the rear panel and to the right of the Ethernet LAN ports.

NOTICE: Only P1 (COM1) port is currently supported by Connect Plus for external serial communications.

Figure 12: RS-232/422/485 Serial Ports (P1-P2)

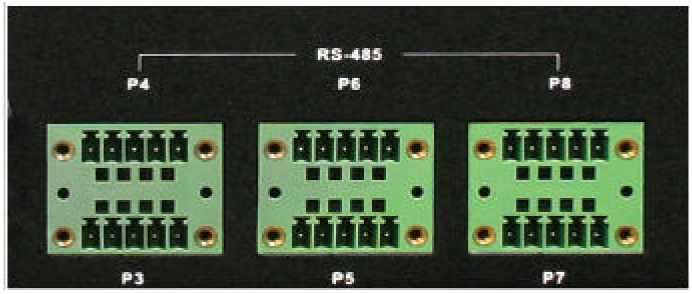


3.3.2.2.6

RS-485 Serial Ports (P3-P8)

The six (6) RS-485 Serial (COM) Ports are labeled P3 through P8. These ports are located on the rear panel and to the right of the P1 and P2 Serial Ports. They are not currently used.

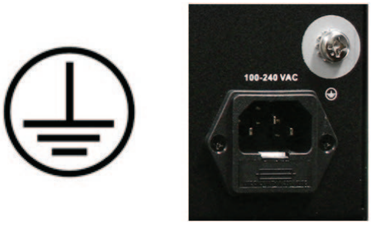
Figure 13: RS-485 Serial Ports (P3-P8)



3.3.2.2.7
Grounding Connection

The device panel provides a screw as a grounding point. The screw is identified with the symbol for Earth Ground and is located above and to the right of the Power Input.

Figure 14: Grounding Connection



3.4
System Connections

This section describes how to connect the device into a Connect Plus system.

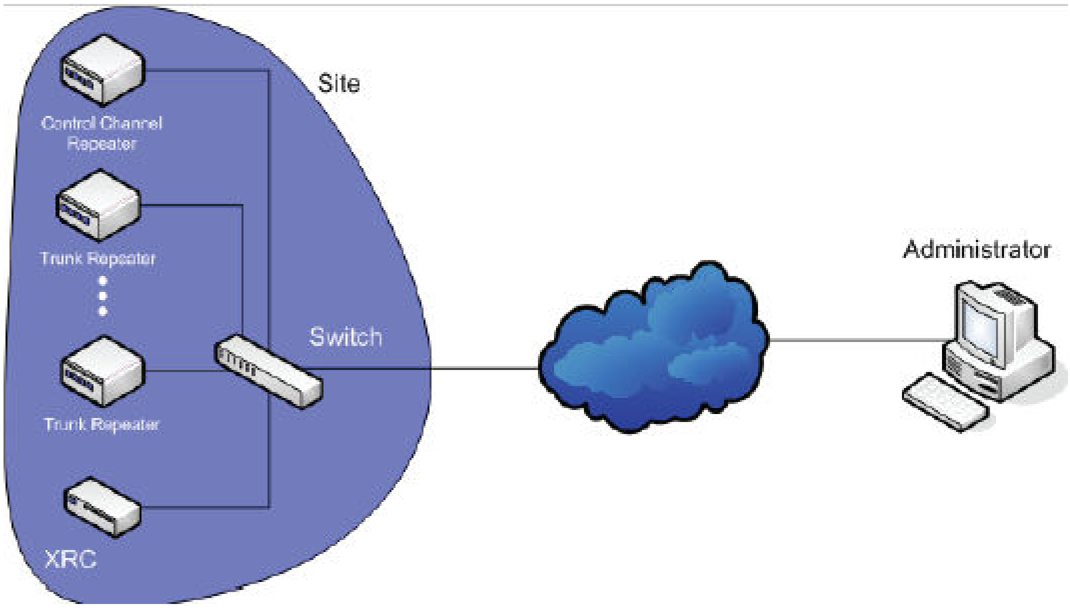
Each Connect Plus site requires at least one XRC Controller. Beginning with Connect Plus Release 1.1, the customer can purchase a second XRC Controller per site to serve as backup to the primary XRC. The secondary controller provides backup capability, but it does not increase the number of repeaters and calls that can be managed per site.

If the site will employ a Redundant Controller configuration, read the "Redundant Controller" section of the *MOTOTRBO Connect Plus System Planner*. In the System Planner, you will find diagrams illustrating connections, important operational information, and the steps that must be followed when configuring and deploying redundant controllers at the site.

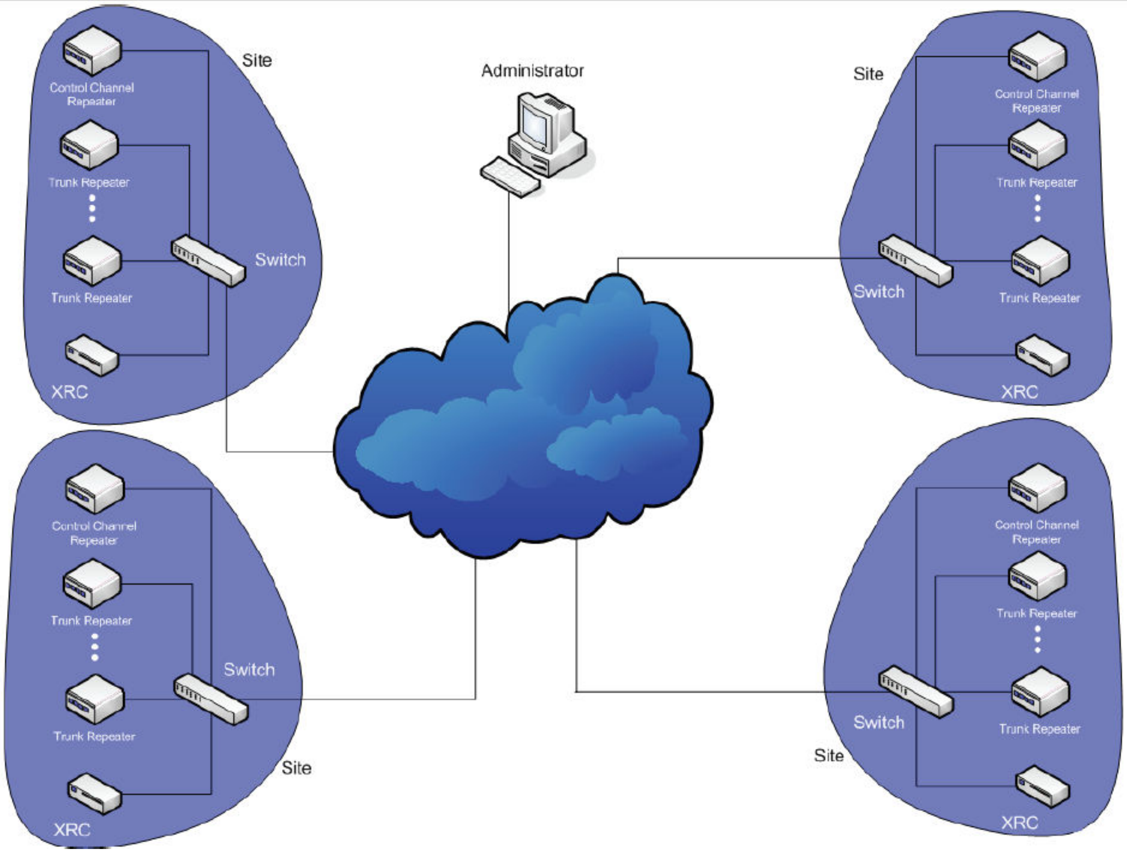
3.4.1
Single Site Block Diagram

The following diagram shows the system connections of the XRC in a single site.

Figure 15: System Connections of the XRC in a Single Site



3.4.2
Multisite Block Diagram



NOTICE: See the *MOTOTRBO Connect Plus System Planner* for more information on network topologies and IP considerations for a Connect Plus Multisite Network.

3.4.3
PC Connection for Initial Configuration

There are multiple methods to connect to the device. The two most common methods are described in the following sections.

- Ethernet Port Connection of the Device on page 43
- Connecting Through the Serial Port of the Device on page 44

3.4.3.1
Ethernet Port Connection of the Device

The Network Parameters of the PC will have to be temporarily changed to match the default Network Parameters of the device. Once the Network Parameters of the device are set for your network, then the Network Parameters of the PC can be returned to their original settings. See PC Connection for Initial Configuration on page 43.

3.4.3.1.1
Connecting to the Device Through an Ethernet Switch

Prerequisites: Minimum switch requirements:

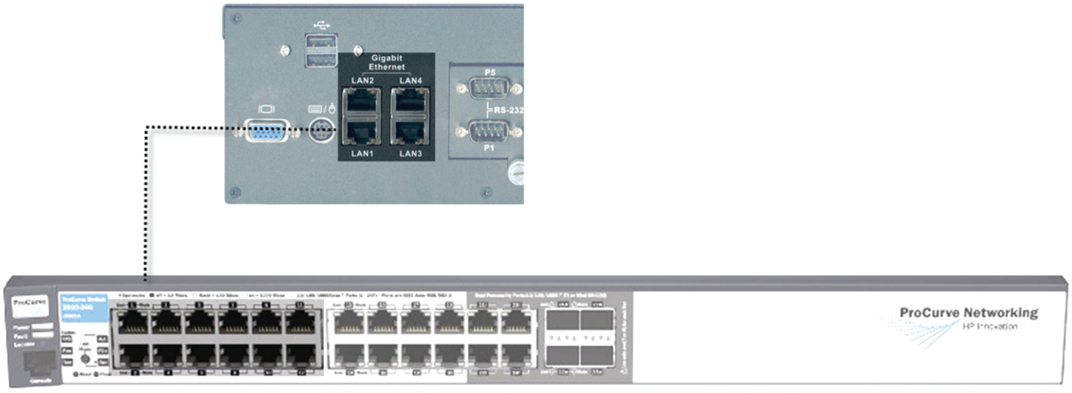
- 100 Mbps ports
- At least 16 ports
- Managed (recommended but not required)
- Capable of accepting gratuitous ARP responses (for sites that incorporate redundant XRC Controllers)

Procedure:

1. Plug one end of a straight-through Category 5 Ethernet cable into the LAN1 port located on the left side of the rear panel of the device.
2. Plug the other end of the cable into any available port on the Ethernet Switch.
3. Plug one end of a straight-through Category 5 Ethernet cable into the LAN port located on the computer running the Network Manager Connection Tool.
4. Plug the other end into the site Ethernet switch.

   The following illustration shows the device connection to an Ethernet Switch. The 9100 model also connects to the LAN Ethernet switch via its LAN1 port.

Figure 16: Device Connection to Ethernet Switch



3.4.3.2 Direct Connection: PC to Device

Plug one end of a Category 5 Ethernet crossover cable into the LAN1 port, located on the left side of the rear panel of the device. Plug the other end of the cable into any available Ethernet port on the PC.

Figure 17: LAN Cable for PC Connection

3.4.3.2.1 Connecting Through the Serial Port of the Device

Procedure:

1. Plug one end of a null modem cable into P1 serial port (COM1 port) located in the middle of the rear panel of the device.
2. Plug the other end of the cable into any available serial port on a Personal Computer.

   Figure 18: Null Modem Cable

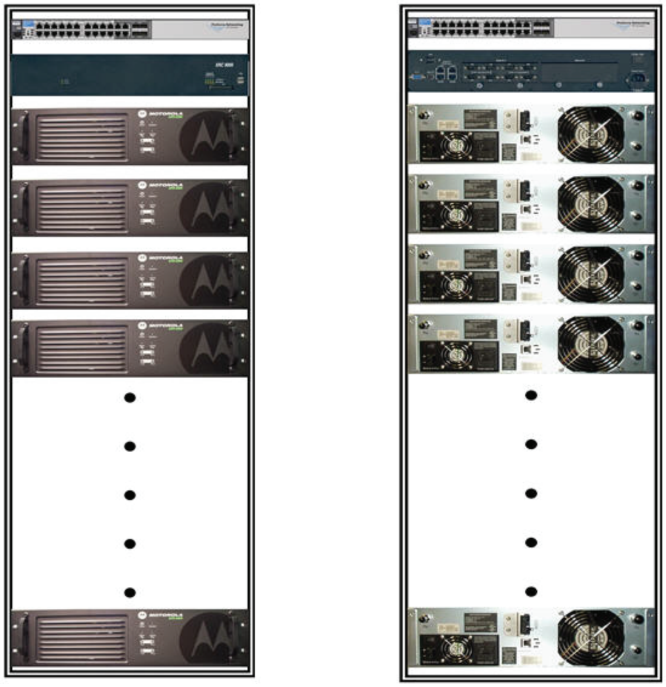
3.4.4 Site Installation

3.4.4.1 Single Site Diagram

The following is an example of rack mounting the components of a single site system. Depending on the installer, the Network Switch can be mounted facing the front or the back of the rack.

NOTICE: The switch can be mounted facing either direction.

Figure 19: Rack Mounting of Components of a Single Site System



3.4.4.2

Power Recommendations

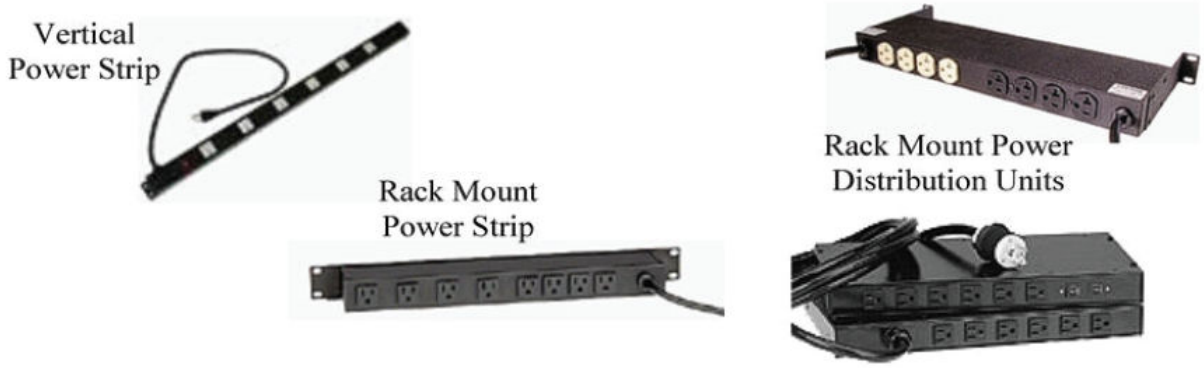
3.4.4.2.1

Primary Power Source

The primary power source can be supplied through the following:

- AC power receptacles (wall sockets)
- Rack mount power distribution unit
- Rack mount power strip
- Vertical power strips

Figure 20: Primary Power Source



3.4.4.2.2 Backup Power Source

Emergency backup power systems usually consist of two components: an Uninterruptible Power Supply (UPS) and a generator. This section only describes the UPS; the selection of the generator is beyond the scope of this document.

A UPS can serve a number of purposes such as filtering out power events, conditioning and providing power if primary power source fails. On the average, the time a UPS is expected to do this, is under five minutes which gives enough time to shut down equipment and for the backup power generator to take over the load.

Depending on your configuration and needs, the following areas require different emphasis:

- Surge Suppression
- Power Conditioning
- Battery Backup

It is strongly recommended that the device and its supporting network equipment (that is, router, switches, consoles, billing collection systems) are backed up by UPS. The 9100 model is a 40 W unit. Check the power requirements of other devices (such as repeaters and network equipment) when calculating the required capacity of a UPS system.

See Appendix A Determining the UPS Capacity on page 187.

3.4.4.2.2.1 Importance of Providing Backup Power

This device is a power-computing device, and like other computers, a power-loss causes the device to lose information not saved to the hard drive or non-volatile memory.

⚠ **CAUTION:** The Roamer lists (where the radio units are presently registered) are kept in volatile memory. This information will be lost if power is interrupted and there is no UPS backup. The loss of this important data can cause a degradation of service until the lists are restored through subsequent registrations.

3.4.4.2.3 Mounting the Device in a Rack

The device can be mounted in a system rack.

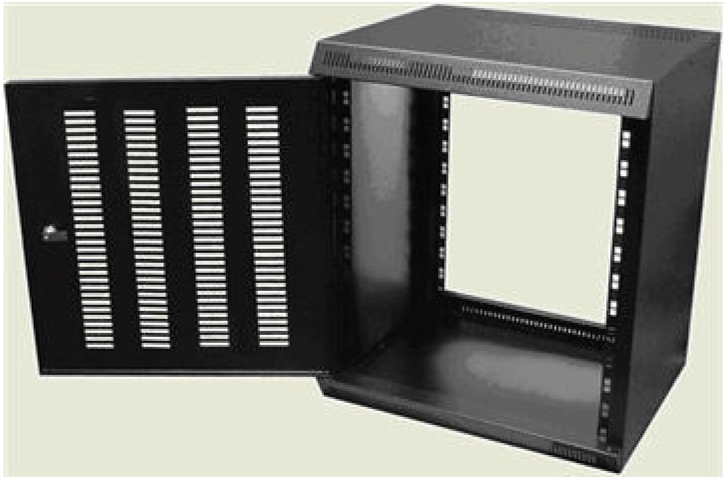
Prerequisites: There are different types of racks, as follows:

- Rails and base only

- Enclosure without a door

- Enclosure without a door on wheels

- Enclosure with a door



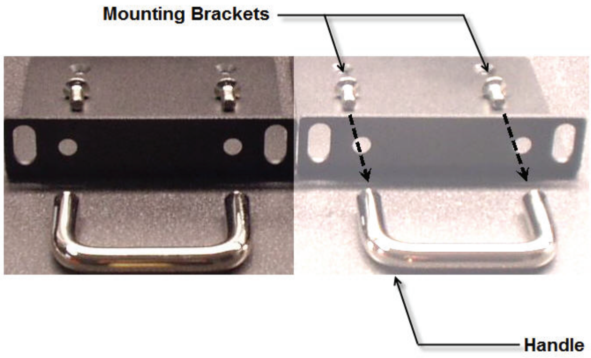
- Enclosure with a glass door

Select the mounting type that is suitable for your environment.

When and where to use:
Context for the current task

Procedure:

1. Using four (4) screws, attach the handles to the mounting brackets by fastening them via the through holes.



2 Install the device in the rack.

3 Adjust the mounting bracket to fit.

Adjustment should not be required for standard EIA racks.

4 Using four rack screws, secure the unit to the mounting rails.

3.4.4.2.4

Connecting the Device to the Ethernet Switch

Procedure:

Connect the device to the switch after mounting it in the rack.

3.4.4.2.5

Connecting the Controller to the MOTOTRBO Repeater(s)

The following sections discuss on configurations of how to connect the XRC Controller to the MOTOTRBO Repeater(s).

3.4.4.2.5.1

Configuring the MOTOTRBO Repeater for Connect Plus Operation

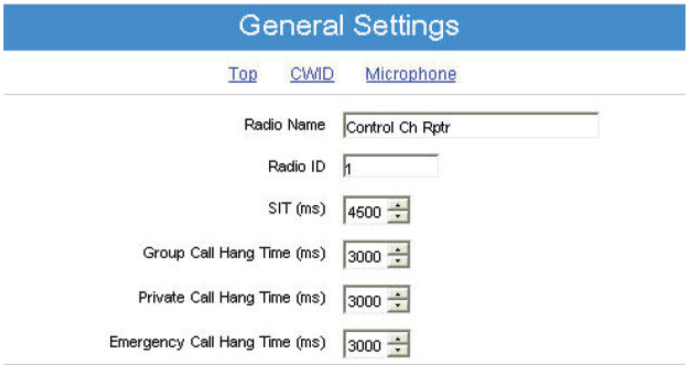
This section addresses only the repeater settings that are critical to Connect Plus operation and assumes that all other parameters have already been set.

3.4.4.2.5.2

MOTOTRBO CPS General Settings

The most important General Settings for Connect Plus are shown in the following figure. The Radio Name field is used to configure an alias for the repeater. The alias can help you identify the codeplug of this repeater, but it is not transmitted over the air. Other General Settings are discussed in the sub-sections that follow.

Figure 21: General Settings Screen



General Settings

Radio Name	Control Ch Rptr
Radio ID	1
SIT (ms)	4500
Group Call Hang Time (ms)	3000
Private Call Hang Time (ms)	3000
Emergency Call Hang Time (ms)	3000

3.4.4.2.5.2.1

Radio ID

This parameter defines the Radio ID of the repeater.

Maximum	15
Minimum	1
Increment	1

Default	Blank

NOTICE: The programmable range is not enforced by MOTOTRBO CPS, but it must be followed for proper Connect Plus operation.

3.4.4.2.5.2.2 Subscriber Inactivity Timer (SIT)

How the repeater uses the Subscriber Inactivity Timer (SIT) programmed with MOTOTRBO CPS depends on which Connect Plus software release is used by the XRC Controller:

- If the XRC software is prior to Connect Plus Release 1.1, the repeater always uses the CPS-configured value, even during Connect Plus operation. Follow the configuration guidelines as described in this section.
- Beginning with Connect Plus Release 1.1, the SIT value that is programmed with MOTOTRBO CPS will be overwritten by the XRC when it establishes its link with the repeater. The SIT value is not programmable in the MOTOTRBO Connect Plus Network Manager, but the XRC does consider other Network Manager-configurable values (the Call Hang Timers) when setting the SIT. The repeater will use the SIT value supplied by the XRC as long as it maintains connectivity to the controller. It is important to know that MOTOTRBO CPS always displays the CPS-configured value, even when connected to the XRC. The repeater utilizes the CPS-configured value when it doesn’t have a connection to the XRC (such as when the repeater is operating in Conventional Fallback mode).

The Subscriber Inactivity Timer (SIT) parameter controls how long the repeater continues transmitting with absence of subscriber activity on the uplink.

The Subscriber Inactivity Timer (SIT) starts when there is no inbound subscriber activity on either time slot (Slot 1 or 2) of a repeater. When the SIT expires, the repeater stops transmitting until awoken again by a subscriber or the XRC.

In order to accommodate the reserved hang time after each transmission, the SIT timer should always be equal to or greater than the longest call hang time in the repeater.

IMPORTANT: The requirement to set this timer the same for all Connect Plus repeaters is not enforced by MOTOTRBO CPS, but it must be followed for proper Connect Plus operation.

Maximum	7000 ms
Minimum	1000 ms
Increment	500 ms

3.4.4.2.5.2.3 Group Call Hang Time (ms)

How the repeater uses the Group Call Hang Time programmed with MOTOTRBO CPS depends on which Connect Plus software release is used by the XRC Controller:

- If the XRC software is prior to Connect Plus Release 1.1, the repeater always uses the CPS-configured value, even during Connect Plus operation. Follow the configuration guidelines as described in this section.
- Beginning with Connect Plus Release 1.1, the Group Call Hang Time value that is programmed with MOTOTRBO CPS will be overwritten by the XRC when it establishes its link with the repeater. In doing so, the XRC uses the Group Call Hang Time value that has been programmed with the MOTOTRBO Connect Plus Network Manager. The repeater will use the Network Manager-configured value as long as it maintains its connection to the XRC. It is important to know that MOTOTRBO CPS always displays the CPS-configured value, even when connected to the XRC.

The repeater utilizes the CPS-configured value when it doesn't have a connection to the XRC (such as when the repeater is operating in Conventional Fallback mode).

This parameter defines the time the repeater reserves the channel for, after the end of a group call transmission. During this time, only members of the Group that the channel is reserved for can transmit. This allows for smoother conversation.

IMPORTANT: The value of this parameter must be equal to or less than the SIT value. Connect Plus recommends the Group Hang Time be set to 3 seconds or longer.

Maximum	7000 ms
Minimum	0 ms
Increment	500 ms

IMPORTANT: The requirement to set this timer the same for all Connect Plus repeaters is not enforced by MOTOTRBO CPS, but it must be followed for proper Connect Plus operation.

NOTICE: The Group Call Inactivity Timer in XRC must be set at least one second longer than the Group Call Hang Time in the repeater.

3.4.4.2.5.2.4 Private Call Hang Time (ms)

How the repeater uses the Private Call Hang Time programmed with MOTOTRBO CPS depends on which Connect Plus software release is used by the XRC Controller:

- If the XRC software is prior to Connect Plus Release 1.1, the repeater always uses the CPS-configured value, even during Connect Plus operation. Follow the configuration guidelines as described in this section.
- Beginning with Connect Plus Release 1.1, the Private Call Hang Time value that is programmed with MOTOTRBO CPS will be overwritten by the XRC when it establishes its link with the repeater. In doing so, the XRC uses the Private Call Hang Time value that has been programmed with the MOTOTRBO Connect Plus Network Manager. The repeater will use the Network Manager-configured value as long as it maintains its connection to the XRC. It is important to know that MOTOTRBO CPS always displays the CPS-configured value, even when connected to the XRC. The repeater utilizes the CPS-configured value when it doesn’t have a connection to the XRC (such as when the repeater is operating in Conventional Fallback mode).

This parameter defines the time the repeater reserves the channel for, after the end of a private call transmission. During this time, only the individuals involved in the call that the channel is reserved for can transmit. This allows smoother conversation. You may want to set a longer hang time than the Group Call Hang Time as an individual tends to take a longer time to reply (talk back) in a Private Call.

IMPORTANT: The value of this parameter must be equal to or less than the SIT value.

Maximum	7000 ms
Minimum	0 ms
Increment	500 ms

IMPORTANT: The requirement to set this timer the same for all Connect Plus repeaters is not enforced by MOTOTRBO CPS, but it must be followed for proper Connect Plus operation.

NOTICE: The Private Call Inactivity Timer in XRC must be set at least one second longer than the Private Call Hang Time in the repeater.

3.4.4.2.5.2.5 Emergency Call Hang Time (ms)

How the repeater uses the Emergency Call Hang Time programmed with MOTOTRBO CPS depends on which Connect Plus software release is used by the XRC Controller:

- If the XRC software is prior to Connect Plus Release 1.1, the repeater always uses the CPS-configured value, even during Connect Plus operation. Follow the configuration guidelines as described in this section.
- Beginning with Connect Plus Release 1.1, the Emergency Call Hang Time value that is programmed with MOTOTRBO CPS will be overwritten by the XRC when it establishes its link with the repeater. In doing so, the XRC uses the Emergency Call Hang Time value that has been programmed with the MOTOTRBO Connect Plus Network Manager. The programmable range provided by the Network Manager is considerably higher than the programmable range provided by MOTOTRBO CPS. The repeater will use the Network Manager-configured value as long as it maintains its connection to the XRC. It is important to know that MOTOTRBO CPS always displays the CPS-configured value, even when connected to the XRC. The repeater utilizes the CPS-configured value when it doesn't have a connection to the XRC (such as when the repeater is operating in Conventional Fallback mode).

Sets the duration the repeater reserves the channel, after the end of an Emergency Call transmission. During this time, only the members of the Emergency Group that the channel is reserved for can transmit. This produces smoother conversation. You may wish to set the Emergency Call Hang Time longer than other call hang timers (so that the repeater will not release the Emergency channel too quickly).

IMPORTANT: The value of this parameter must be equal to or less than the SIT value.

Maximum	7000 ms
Minimum	0 ms
Increment	500 ms

IMPORTANT: The requirement to set this timer the same for all Connect Plus repeaters is not enforced by MOTOTRBO CPS, but it must be followed for proper Connect Plus operation.

NOTICE: The Emergency Call Inactivity Timer in XRC must be set at least one second longer than the Emergency Call Hang Time in the repeater.

3.4.4.2.5.2.6 Continuous Wave Identification (CWID)

If this radio must send CWID (Continuous Wave Identification) in order to fulfill the FCC requirements, enter the ID in this field.

For normal Connect Plus operation, the radio ignores the TX Interval programmed with MOTOTRBO CPS. The TX interval for this repeater must be set in the XRC. For Connect Plus Auto Fallback operation, the repeater uses the interval programmed with MOTOTRBO CPS.

3.4.4.2.5.2.7 TX Power Settings

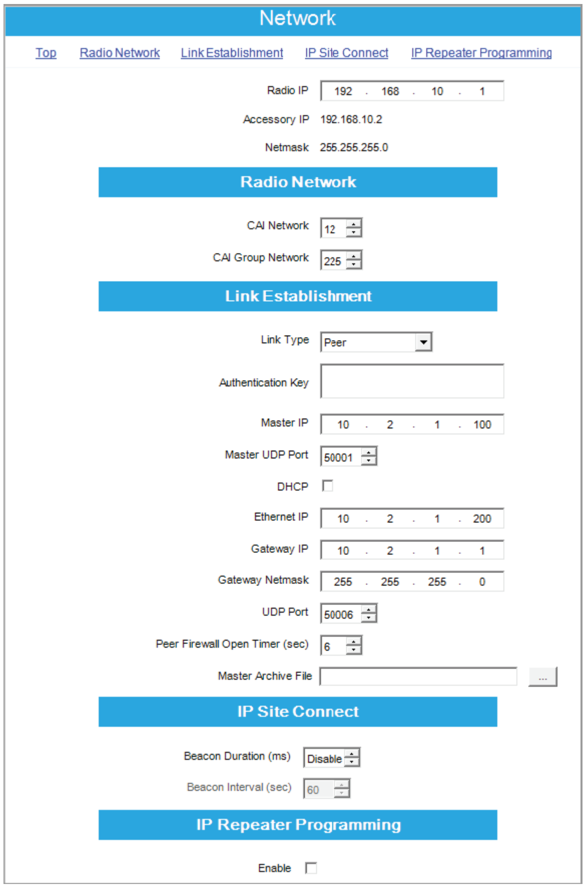
Radio Power Settings should be set the same for all repeaters in the same site. This is because all repeaters in the same site must have the same coverage footprint.

3.4.4.2.5.3 MOTOTRBO CPS Network and Link Establishment Settings

Using the MOTOTRBO CPS, connect to the MOTOTRBO repeater and set the following parameters:

- Link Type
- Beacon Duration
- Master IP
- Master UDP Port
- DHCP
- Ethernet IP
- Gateway IP
- Gateway Netmask
- Enable IP Repeater Programming (32 MB repeaters)

Figure 22: Network Settings and Link Establishment Settings Screen



Network

Top | Radio Network | Link Establishment | IP Site Connect | IP Repeater Programming

Radio IP: 192 . 168 . 10 . 1
Accessory IP: 192.168.10.2
Netmask: 255.255.255.0

Radio Network

CAI Network: 12
CAI Group Network: 225

Link Establishment

Link Type: Peer
Authentication Key:
Master IP: 10 . 2 . 1 . 100
Master UDP Port: 50001
DHCP: □
Ethernet IP: 10 . 2 . 1 . 200
Gateway IP: 10 . 2 . 1 . 1
Gateway Netmask: 255 . 255 . 255 . 0
UDP Port: 50006
Peer Firewall Open Timer (sec): 6
Master Archive File: ...

IP Site Connect

Beacon Duration (ms): Disable
Beacon Interval (sec): 60

IP Repeater Programming

Enable: □

Except for IP addresses, port numbers, and DHCP settings (which can vary according to customer needs), your settings should be as shown in the figure. Depending on your repeater firmware and MOTOTRBO CPS software version, the settings may not appear in the same order as shown in the figure, or as listed in the subsections that follow. The network settings and link establishment settings may appear on the same screen, or on separate screens.

3.4.4.2.5.3.1 Configuring the Link Type

This parameter configures the link type.

Procedure:

Select **Peer** for Connect Plus operation.

3.4.4.2.5.3.2 Configuring the Master IP

This is a radio-wide parameter. The format and range for the address are *`<000-255>.<000-255>.<000-255>.<000-255>`*.

Procedure:

Enter the IP address of the XRC to identify the XRC as the Master.

3.4.4.2.5.3.3 Master UDP Port

This is a radio-wide parameter that specifies the User Datagram Protocol (UDP) port number of the Master within the system. UDP is a protocol used for peer-to-peer services within the system.

Each repeater in the site must be programmed with a unique number for Master UDP Port. The number must fall between the value for First UDP Repeater Listen Report (a programmable XRC parameter) and First Repeater Listen Port +14.

Maximum	65535
Minimum	1024
Increment	1

NOTICE: The minimum usable value for Connect Plus is 4000. This is because the minimum value for “First UDP Repeater Listen Port” in the XRC controller is 4000.

3.4.4.2.5.3.4 DHCP

Dynamic Host Configuration Protocol (DHCP) enables dynamic IP address allocation for the peer repeater. This is a radio-wide parameter.

NOTICE: The value of this parameter is not preserved during cloning and is disabled (unchecked) after any clone operation.

3.4.4.2.5.3.5 Ethernet IP

This is a radio-wide parameter that assigns an Ethernet IP Address for the repeater. The format and range for the address are (000-255).(000-255).(000-255).(000-255). Assign Ethernet IP so the number is a unique IP address.

The field is grayed out when DHCP is enabled.

3.4.4.2.5.3.6 Gateway IP

This is a radio-wide parameter that assigns a Gateway IP Address for the Peer repeater. The format and range for the address are ***<000-255>.<000-255>.<000-255>.<000-255>***. Assign Gateway IP so number is a unique IP address.

The field is grayed out when DHCP is enabled.

NOTICE: Out of network messages are forwarded to the Gateway node.

3.4.4.2.5.3.7 Gateway Netmask

This is a radio-wide parameter that assigns a Gateway Netmask Address for the Peer repeater. Assign Gateway Netmask to the Gateway Netmask address.

The field is grayed out when DHCP is enabled.

NOTICE: Gateway Netmask determines which IP addresses are considered "in network" or "out of network".

3.4.4.2.5.3.8 Configuring the UDP Port

Procedure:

Leave at the default value for Connect Plus operation.

3.4.4.2.5.3.9 Configuring Peer Firewall Open Timer (sec)

Procedure:

For Connect Plus operation, leave at the default value.

3.4.4.2.5.3.10 Beacon Duration (ms)

This is a radio-wide parameter that configures the length of the beacon signal. For Connect Plus operation, select **Disabled** or **0**.

3.4.4.2.5.3.11 Setting the CAI Network

Procedure:

For Connect Plus operation, set to `12`.

3.4.4.2.5.3.12 Setting the CAI Group Network

Procedure:

For Connect Plus operation, set to `255`.

3.4.4.2.5.3.13 Enabling IP Repeater Programming

This enables properly authorized users to perform MOTOTRBO CPS programming of this repeater via the IP network. The checkbox appears for 32 MB repeaters only. Remote repeater programming requires an operational Connect Plus site controller and an operable site LAN. IP Repeater Programming is a purchasable feature for MOTOTRBO CPS. For a more detailed discussion of IP Repeater Programming, see the *MOTOTRBO Connect Plus System Planner*.

Procedure:

Check this box to enable the remote repeater programming feature.

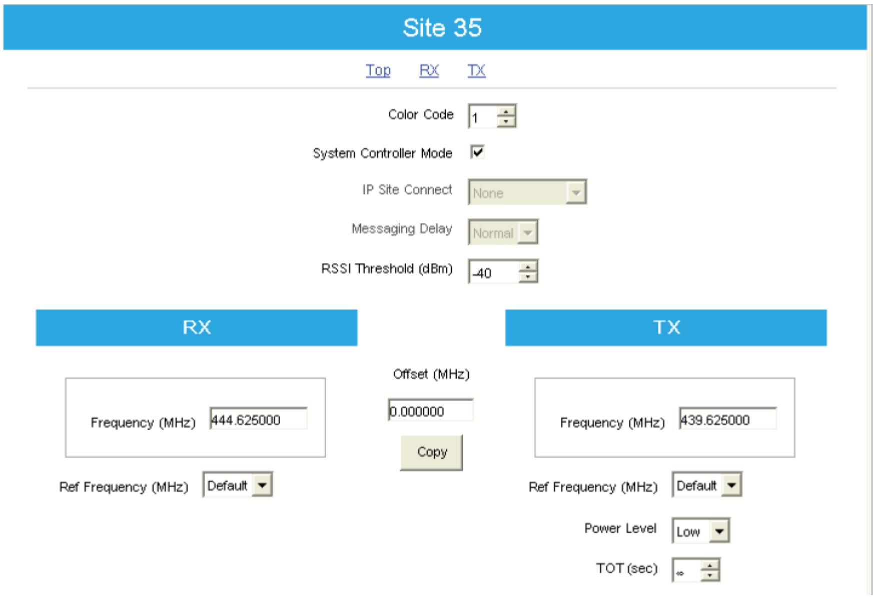
3.4.4.2.5.4 MOTOTRBO CPS Channel Settings

Using MOTOTRBO CPS, connect to the MOTOTRBO repeater. In the Channel screen, set the following parameters:

- Color Code
- IP Site Connect
- Message Delay
- RSSI Threshold
- RX Frequency
- RX Ref Frequency
- TX Frequency
- TX Ref Frequency
- TX Power Level
- TX TOT

The following figure shows the Channel Settings. Most of these settings are configured per the customer's requirements as discussed in the following sections.

Figure 23: Channel Settings Screen



Color Code: 1

System Controller Mode: ☑

IP Site Connect: None

Messaging Delay: Normal

RSSI Threshold (dBm): -40

Offset (MHz): 0.000000

RX Frequency (MHz): 444.625000

RX Ref Frequency (MHz): Default

TX Frequency (MHz): 439.625000

TX Ref Frequency (MHz): Default

Power Level: Low

TOT (sec): ∞

3.4.4.2.5.4.1 Color Code

This is a radio-wide parameter that allows a color code to be assigned to a given channel. Channels may have the same or different color codes. A repeater can only have one color code.

In Connect Plus, a color code is used to identify a specific repeater and frequency pair. Repeaters in the same Connect Plus site may be assigned the same Color Code, or different Color Codes, depending on frequency management considerations discussed in this paragraph. Repeaters in the same Connect Plus site must all have unique frequency pairs. Frequencies may be re-used at different Connect Plus sites, provided that coverage does not overlap for the re-used frequencies. If the coverage does not typically overlap, but may overlap in unusual RF conditions (such as when the SU is in a very high spot), the two repeaters that share the same frequency should be assigned different color codes. This helps the subscriber units to distinguish between the two repeaters, especially while roaming. Additionally, on shared channels, spectrum regulators may wish to assign different color codes to different licensees as part of their license agreement.

Maximum	15
Minimum	0
Increment	1

IMPORTANT: Color Code must match the configuration for the Radio ID and frequency pair (for this site) in the Connect Plus Network Frequency File.

3.4.4.2.5.4.2 System Controller Mode

The System Controller Mode checkbox is introduced in MOTOTRBO Repeater Firmware Release 2.3. It is grayed out (not available) until the IP Site Connect Plus setting is set to "None". System Controller Mode must be enabled before the repeater can be used as a Connect Plus resource.

3.4.4.2.5.4.3 Configuring for IP Site Connect

Configuration for this setting depends on the repeater's firmware level.

Procedure:

Perform one of the following actions:

- If the repeater firmware is MOTOTRBO Repeater Firmware Release 2.3 or later, set IP Site Connect to **None** and check the **System Controller Mode** checkbox.
- If the repeater firmware is prior to MOTOTRBO Repeater Firmware Release 2.3, set IP Site Connect to **Slots 1 and 2**.

3.4.4.2.5.4.4 Messaging Delay (ms)

If the repeater firmware is MOTOTRBO Repeater Firmware Release 2.3, or later, the Messaging Delay entry box is grayed out when **System Controller Mode** is enabled.

If the repeater firmware is prior to MOTOTRBO Repeater Firmware Release 2.3, leave **Messaging Delay** at the default setting of **Normal**.

3.4.4.2.5.4.5 RSSI Threshold (dBm)

This threshold is used to measure the maximum interference signal that the repeater tolerates.

If the repeater detects an interfering signal at or above this threshold, it takes itself off-line and reports its off-line condition to the XRC. If the Control Channel repeater were to take itself off-line, site operations would be severely impacted. For this reason the interference threshold for the Control Channel repeater should be set to a high value (in the range of -80 to -40 dBm).

Connect Plus Control Channel frequency pairs require a Protected Service Area. Non-exclusive licenses such as FB2 or FB6 are not suitable for Connect Plus Control Channel operation. This is a channel-wide feature.

Maximum	-40 dBm
Minimum	-130 dBm
Increment	1 dBm

3.4.4.2.5.4.6 RX Frequency (MHz)

This parameter allows the user to enter a receive (RX) frequency for the repeater.

IMPORTANT: Must match the RX Frequency configured for this Radio ID and site in the Connect Plus Option Board Network Frequency File.

3.4.4.2.5.4.7 RX Ref Frequency (MHz)

This is a channel-wide parameter that selects the Reference Frequency used when receiving on the current channel. The reference frequency can be shifted to allow the radio to operate on channel frequencies that would otherwise be blocked by internally generated spurious signals. Internally generated spurious signals would appear as silent carriers on certain channel frequencies. Shifting the reference frequency allows these permanent signal carrier to be shifted to unused frequencies so that the desired channel frequencies can still be used.

The options for UHF radios are: Default, 5.6MHz or 8.4MHz. For VHF band radios, the options are: Default, 3.36MHz or 4.2MHz. For other bands radios, the option is set to Default and is not MOTOTRBO CPS programmable.

The radio as it is shipped is compliant with all RTTE regulations. Changing the reference to these frequencies will impact the radio's performance specifications and could result in non-compliance with the RTTE requirements. Conformity to the local regulatory standards must be verified by the person/ organization applying this change.

3.4.4.2.5.4.8 TX Frequency (MHz)

This parameter allows the user to enter a transmit (TX) frequency for the repeater.

IMPORTANT: This parameter must match the TX frequency configured for this Radio ID and site in the Connect Plus Option Board Network Frequency File.

3.4.4.2.5.4.9 TX Ref Frequency (MHz)

This is a channel-wide parameter that selects the Reference Frequency used when transmitting on the current channel. The reference frequency can be shifted to allow the radio to operate on channel frequencies that would otherwise be blocked by internally generated spurious signals. Internally generated spurious signals would appear as silent carriers on certain channel frequencies.

Shifting the reference frequency allows these permanent signal carrier to be shifted to unused frequencies so that the desired channel frequencies can still be used.

- The options for UHF radios are: **Default**, **5.6MHz** or **8.4MHz**.
- For VHF band radios, the options are: **Default**, **3.36MHz** or **4.2MHz**.
- For other band radios, the option is set to **Default** and is not MOTOTRBO CPS programmable.

The radio as it is shipped is compliant with all RTTE regulations. Changing the reference to these frequencies will impact the radio's performance specifications and could result in non-compliance with the RTTE requirements. Conformity to the local regulatory standards must be verified by the person/ organization applying this change.

NOTICE: The RX Only must be disabled.

3.4.4.2.5.4.10
TX Power Level

This parameter sets the system's transmission power level. Available options are:

High
Used when a stronger signal is needed to extend transmission distances.

Low
Used when communicating in close proximity, and to prevent transmissions into other geographical groups.

IMPORTANT: All repeaters for this site should have the same power and coverage footprint.

3.4.4.2.5.4.11
Time-Out Timer (sec)

The Time-Out Timer (TOT) parameter of the Repeater must not be set any shorter than the longest TOT in any Connect Plus SU or other transmitting device (such as a wireline console or other XRT Client).

Maximum	495, ∞ sec
Minimum	15 sec
Increment	15 sec

NOTICE: Time-out timer is disabled if the Infinity (∞) option is selected.

CAUTION: Chassis may get warm to touch if Time-Out Timer for the current channel is set to Infinity (∞) and continuous PTT for more than 15 minutes.

3.4.4.2.5.4.12
Other Channel Settings

Depending on device features, hardware, and repeater firmware level, other channel settings may be displayed.

Procedure:

Perform the following actions:

- If the **Phone Gateway** setting is displayed, set to **None** for Connect Plus operation.
- If the **IF Filter Type** setting is displayed, refer to MOTOTRBO CPS Help for information.
- If the **BSI Mode** setting is displayed, set to **Analog** or **Digital**.

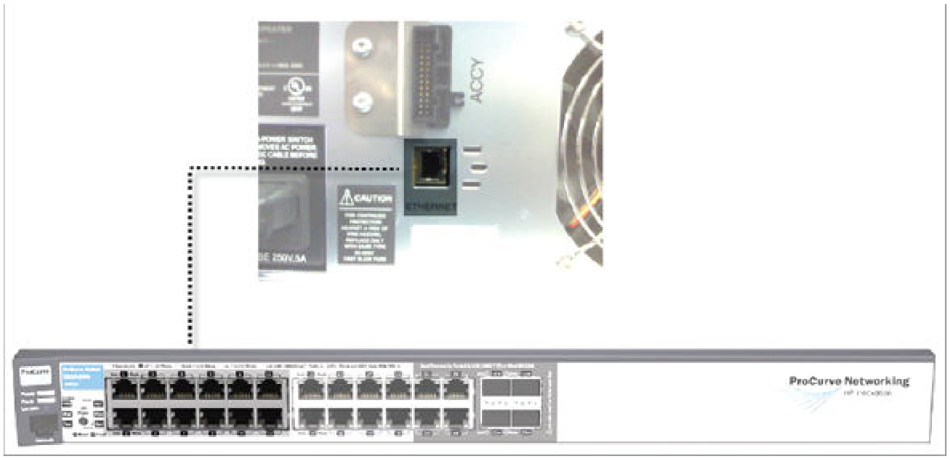
3.4.4.2.5.5 Connecting the MOTOTRBO Repeater(s) to an Ethernet Switch

Procedure:

1. Plug one end of a straight-through Category 5 Ethernet cable into the Ethernet port of the repeater.
2. Plug the other end of the cable into any available Ethernet port on the Ethernet switch.

   The following example shows an HP Procurve 2800 Series Switch.

   Figure 24: Example of Ethernet Switch



Chapter 4

Communicating with the Device

This chapter describes the communication with the device after physical installation and after electrical connections are in place.

Before proceeding, ensure that all the connections are still in place and secure.

4.1

Configuring the PC Network for Initial Configuration

To establish a link between the PC and the device, the Network Parameters of the PC have to be configured in order for the MOTOTRBO Connect Plus Network Manager Connection Tool to be able to communicate with the device through the Ethernet port.

Prerequisites: The following procedure is for Microsoft® Windows Vista™ operating system. For other operating systems, consult your IT department.

Procedure:

1. From the **Start** menu select the **Control Panel**.
2. Select **Network and Internet.**
3. Select **Network and Sharing Center**.
4. Click **Manage network connections**.
5. Select **Local Area Connection** from the list.
6. From the sub-menu, select **Change settings of this connection**.

   The Local Area Connection Properties window appears.
7. Select **Internet Protocol Version 4 (TCP/IPv4)** connection and click the **Properties** button.

   The Internet Protocol (TCP/IP) Properties window appears.
8. Select the **Use the following IP address** radio button and enter the following information:

   IP address: 192.168.1.16 (192.168.1.15 is the default XRC IP address)

   Subnet mask: 255.255.255.0

   Default gateway: 192.168.1.1
9. Click the **OK** button to return to the Local Area Connection Properties window.
10. Click the **OK** button in the Local Area Connection Properties window to complete the PC Network Communications setup.

4.2

Connect Plus Network Manager Connection Tool Software

Microsoft .NET Framework Requirement: A PC can (and frequently does) have multiple versions of Microsoft .NET Framework. To utilize Network Manager versions prior to Connect Plus System Release 1.3, the PC must have at least one of the following .NET Framework versions: 2.0, 3.0 or 3.5.

To utilize a Network Manager version for Connect Plus System Release 1.3 (or later), the PC must have .NET Framework version: 4.0. To see what versions are on your PC, check **Control Panel** → **Add or Remove Programs**.

4.2.1 Installing MOTOTRBO Connect Plus Network Manager Connection Tool on the PC

Prerequisites: Download the Installation folder from Motorola Online (MOL). The folder includes two (2) files:

Setup.exe
This is the application that is used to install the MOTOTRBO Connect Plus Network Manager Connection Tool software on your PC.

MOTOTRBO Connect Plus Network Manager Connection Tool Setup.msi
Microsoft Windows Installation file.

Procedure:

1. From the Installation folder, double-click the `setup.exe` file.
2. Answer the questions and follow the prompts provided by the Installation Wizard.

   The Installation Wizard provides a message when installation is complete.
3. Follow the prompt to close the message and to exit the Installation Wizard.

4.2.2 Launching the MOTOTRBO Connect Plus Network Manager Connection Tool Software

When and where to use:

⚠ **CAUTION:** Do not open more than one instance of the MOTOTRBO Connect Plus Network Manager Connection Tool on the same computer, as this can result in unexpected and undesirable operation.

Procedure:

Launch the MOTOTRBO Connect Plus Network Manager Connection Tool Software through one of the following applications:

- **Desktop Icon**

Double-click on the icon shown as follows. The Setup Wizard creates an icon on the Desktop that is a shortcut to the MOTOTRBO Connect Plus Network Manager Connection Tool Application during installation.

- **Start Menu**

To run the MOTOTRBO Connect Plus Network Manager Connection Tool application through the Start menu, select **Start** → **All Programs** → **Motorola Solutions** → **MOTOTRBO Connect Plus Network Manager Connection Tool**.

- **Program Files Folder**

To run the MOTOTRBO Connect Plus Network Manager Connection Tool Application through the `Program Files` folder, navigate to the Program Files folder, open the `Motorola Solutions` folder, locate and open the `MOTOTRBO Connect Plus Network Manager Connection Tool` folder, and then double-click `MOTOTRBO Connect Plus Network Manager Connection Tool.exe`.

4.2.3 Establishing Connection with the Device

4.2.3.1 Powering Up the Device

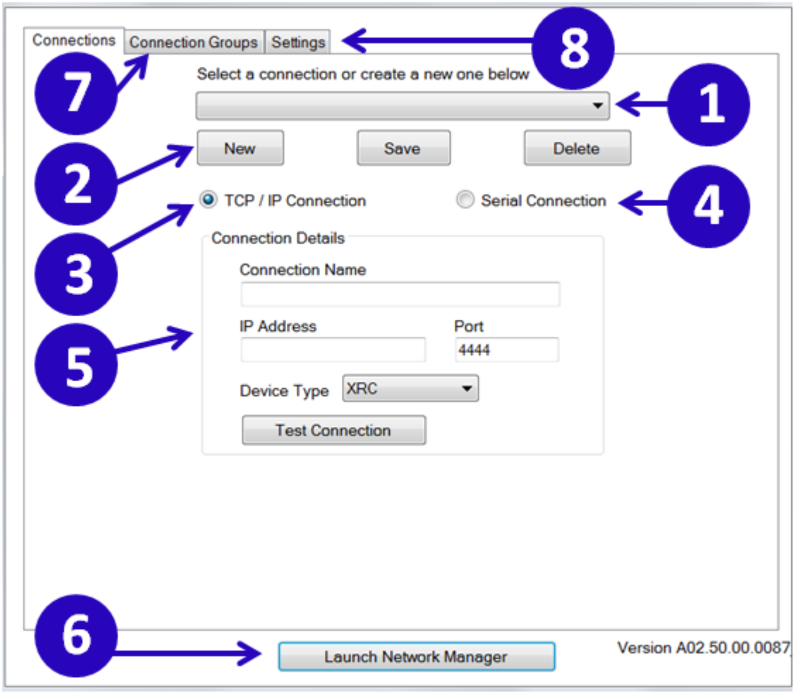
Once the power cord is installed and power is applied the device will boot-up. The On/Off switch does not need to be pressed. This is the operation when the unit has not been connected to power, and then power is applied. Normal power-up (when there has been no loss of power) is accomplished with a momentary press of the On/Off switch.

To manually turn off the unit: If the On/Off switch is pressed with a short press, the unit powers down normally, which can take up to 30 seconds. This is the recommended method for powering down. If the On/Off switch is pressed with a long press (about 10 seconds) then the unit immediately shuts down. Immediate shutdown (long press of the On/Off switch) should only be used if the normal power-down is unsuccessful, as recent changes may be lost.

4.2.3.2 MOTOTRBO Connect Plus Network Manager Connection Tool

The MOTOTRBO Connect Plus Network Manager Connection Tool program is used to connect your PC to the XRI Interconnect Gateway and/or the XRC controller. Upon connecting to the XRI or XRC, the Network Manager Connection Tool starts the MOTOTRBO Connect Plus Network Manager, the software program that is used to monitor and configure the XRC controller and the XRI.

Figure 25: MOTOTRBO Connect Plus Network Manager Connection Tool Software



● TCP / IP Connection   ○ Serial Connection

Port: 4444

Device Type: XRC

Version A02.50.00.0087

1 Saved Connection Drop-down Box

2 Connection List Controls

3 Selects TCP / IP Connection

4 Selects Serial Connection

5 Connection Detail Panel

6 Make Connection with the device

7 Connection Groups Tab

8 Settings Tab

4.2.3.3 Connection Setup

Before a connection can be made to an XRI Interconnect Gateway or an XRC Controller, a connection must be created to define the connection type (TCP/IP or serial), and to enter the Connection Details.

Once a Connection has been created, the Connection Tool is ready to attempt a connection to the desired device. When multiple connections have been defined, the Connection Tool can be used to create Connection Groups, which provide the ability to simultaneously connect to multiple Connect Plus sites.

The following sections describe the procedure for creating individual connections, and then describe how multiple individual connections can be placed into a Connection Group.

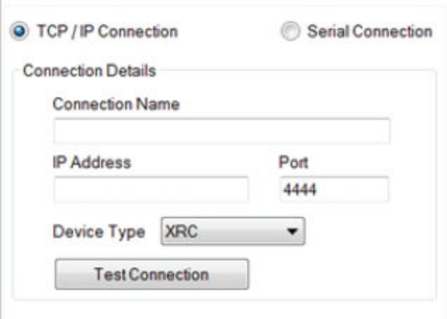
4.2.3.3.1 Connection Detail Panel

The following sections describe each field found in the MOTOTRBO Connect Plus Network Manager Connection Tool Software window in detail.

4.2.3.3.1.1 TCP / IP Connection

When the TCP / IP Connection radio button is selected, the Connection Details screen displays the following fields.

Figure 26: TCP / IP Connection Settings Screen



● TCP / IP Connection ○ Serial Connection

Connection Details

Connection Name

IP Address

Port: 4444

Device Type: XRC

4.2.3.3.1.1.1 Connection Name

This field is used to name the connection.

There is a 255 maximum byte limit for this field. Typically, there will be at least one saved connection per device. In some cases, there may be more than one saved connection per device. For example, there might be separate connections for `Site 1 IP Connection` and `Site 1 Modem Connection`.

NOTICE: If you are not saving the connection settings, then this field is not required.

4.2.3.3.1.1.2 IP Address

This field is used for the IP address of the device for this connection.

Enter the IP address of the device from the perspective of this PC. The format and range for the address are (000-255).(000-255).(000-255).(000-255).

4.2.3.3.1.1.3 Port

This field is used for the MOTOTRBO Connect Plus Network Manager port of the device for this connection.

The default port number is always 4444.

The only exception is when this connection is going through a router utilizing port forwarding, and the router is configured to accept a different port number, and then to convert it to port 4444.

Minimum	1
Maximum	65535
Increment	1
Default	4444

4.2.3.3.1.1.4 Selecting a Device Type

Procedure:

Perform one of the following actions:

- If this connection is for an XRC Controller, select **XRC** as the Device Type.
- If this connection is for an XRI Interconnect Gateway, select **XRI** as the Device Type.

4.2.3.3.1.1.5 Testing Connection

Procedure:

Use this button to test the TCP / IP settings.

- If settings connect to a XRC Controller or XRI Interconnect Gateway, then `Success!` is displayed.
- If the settings do not connect to a XRC Controller or XRI Interconnect Gateway, then `Failed!` is displayed.

4.2.3.3.1.2 Serial Connection

When the Serial Connection radio button is selected, the Connection Details screen displays the following fields:

- Connection Name
- Com Port

- Baudrate
- Device Type
- Phone Number (when Dial modem is enabled)

4.2.3.3.1.2.1 Connection Name

This field is used to name the connection.

There is a 255 maximum byte limit for this field. Typically, there will be at least one saved connection per device. In some cases, there may be more than one saved connection per device. For example, there might be separate connections for `Site 1 IP Connection` and `Site 1 Modem Connection`.

NOTICE: If you are not saving the connection settings, then this field is not required.

4.2.3.3.1.2.2 Selecting a Com Port

This field is used to select communication port of the computer (Com Port).

Procedure:

Click the down arrow and select the appropriate Com Port. If utilizing a modem rather than a direct serial connection to the XRC or XRI, this is the Com Port that has been assigned to the modem.

4.2.3.3.1.2.3 Baudrate - Direct Connection

When used with a direct serial connection this field defines the Com Port baud rate. The MOTOTRBO Connect Plus Network Manager Connection Tool / MOTOTRBO Connect Plus Network Manager is optimized for the default setting of 57600 for the XRC Controller serial connection and 115200 for the XRI Interconnect Gateway serial connection.

NOTICE: For direct serial connection utilizing a null modem cable, it is advised not to change this setting from its default value.

4.2.3.3.1.2.4 Baudrate - Modem Connection

When used with a serial modem this field is used to select the Com Port baud rate to communicate with a modem. The baud rate utilized depends on the following:

- The capabilities and configuration of the two modems involved in the connection.
- The quality of the phone line to the site.

Any speed between 9600 to 57600 is supported, but the lower the speed the slower the communication between the computer and the XRC. Lower speeds will cause delays in updating the screens and information may be missed on the Real Time Display.

4.2.3.3.1.2.5 Modem Details

If a serial modem is being used then check the Dial Modem checkbox and enter the telephone number of the site’s modem. This box will support AT modem commands to allow custom commands required by the modem to be sent.

For example, if the user telephone system required the number 9 and a pause before the telephone number then enter the number in the following format: `9,(`***`<xxx>`***`)`***`<yyy-zzzz>`***

- `9` accesses an outside line
- `,` (comma) causes a pause
- ***`<xxx>`*** is the area code
- ***`<yyy-zzzz>`*** is the telephone number

Check your modem’s documentation for further information.

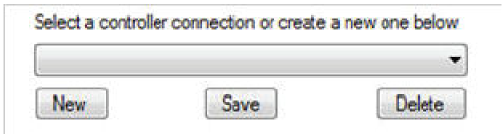
4.2.3.3.1.2.6
Test Com Port

This button is used to test the serial settings.

- If settings connect to a XRC Controller or XRI Interconnect Gateway, then `Success!` is displayed.
- If the settings do not connect to a XRC Controller or XRI Interconnect Gateway, then `Failed!` is displayed.

4.2.3.4
Connection Settings Configuration

Figure 27: Connection Settings Screen



Connection settings to an individual device can be saved in order to speed up connection time in the future (by not having to repeat the initial set-up). In some cases, the technician may want to create and save more than one connection for the same device. This is helpful, for example, when the technician wants to change between a TCP/IP and a serial connection.

For TCP/IP connections, it is possible that the technician may use different IP addresses to connect to the same device, depending on where the technician and the laptop are located. This is another case where the technician may want to create and save multiple connections for the same device.

4.2.3.4.1
Creating and Saving a New Connection

Procedure:

1. Click **New** in Connection List Controls.

   The **Connection Details** Panel is cleared, and TCP / IP will be selected as default.

2. Click either **TCP / IP** or **Serial** to select the connection type.
3. Enter **Connection Name** and fill in the remaining fields for that connection.
4. When all settings are entered, click **Test Connection** to verify the connection is valid.
5. Click **Save** in Connection List Controls.

4.2.3.4.2 Editing an Existing Connection

Procedure:

1. Select the desired connection from the list at the top of the **Connections** tab.

   In **Connection Details** the information for TCP / IP will be displayed as default.
2. Click **Serial** if those settings are to be changed; if not, go to the next step.
3. Change the **Connection Name** or other setting that needs to be changed.
4. Click **Test Connection** to verify that the connection is valid.
5. Click **Save** in the Connection List Controls.

4.2.3.4.3 Deleting a Connection

Procedure:

1. Click on **Select a connection** or create a new one below the drop down box.
2. Select the desired connection.
3. Click **Delete** in Connection List Controls.

4.2.3.5 Launching MOTOTRBO Connect Plus Network Manager Program

When and where to use:

IMPORTANT: Do not open more than one instance of the MOTOTRBO Connect Plus Network Manager on the same computer, as this can result in unexpected and undesirable operation. The XRC can support up to two Network Manager connections at the same time. If multiple users are connected at the same time, changes should be made with caution.

Procedure:

1. Perform one of the following:
   - From the drop-down list, select the desired connection and proceed to step 4.
   - Click the **New** button in Connection List Controls.
2. Select the connection type.
3. Enter connection name and fill in the remaining fields for that connection.
4. Click the **Launch Network Manager** button.
5. Enter the username and password for the site, then click the **Login** button.

   The initial username is `admin`, and the initial password is `admin`.

   A Connection Status window briefly appears, showing the status of the connection. If the wrong User Name or password was entered then an error message appears. If the password authentication is successful, the Network Manager Connection Tool starts the MOTOTRBO Connect Plus Network Manager, the software program that is used to monitor and configure the XRC controller. If this is a first connection (or if the PC has an outdated copy of the Network Manager), the Network Manager Connection Tool will first have to download the latest copy of the MOTOTRBO Connect Plus Network Manager software from the controller. This is an automatic process, and the only indication to the user is the brief appearance of a download bar.

Once the MOTOTRBO Connect Plus Network Manager has been successfully launched, the Site Dashboard displays.

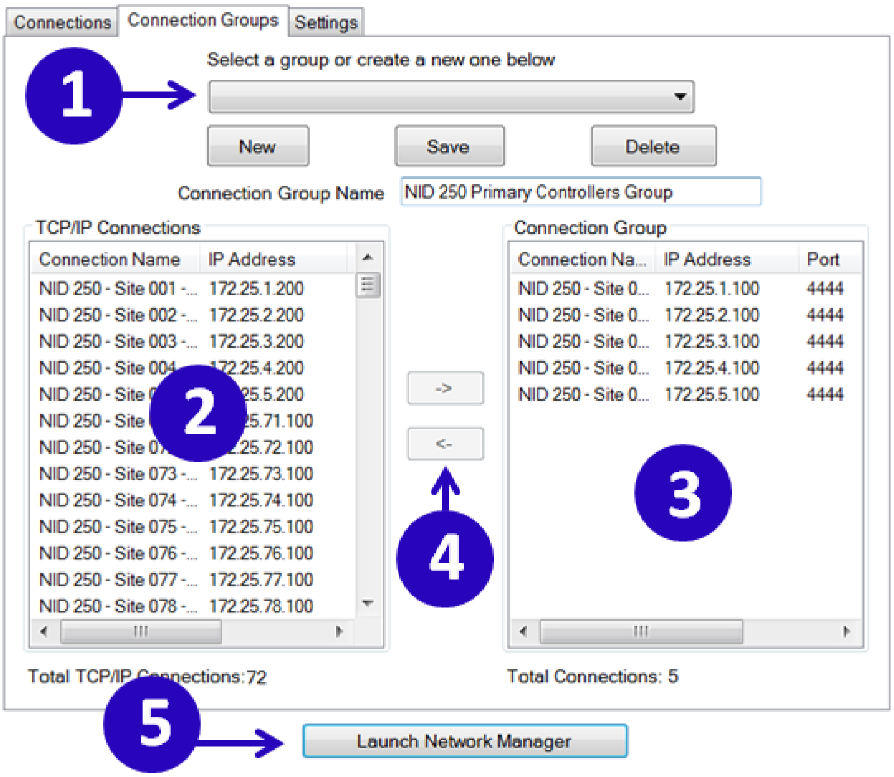
NOTICE: If multiple user connections are required, refer to User Roles in Administrator on page 157 for information on limiting access to features in the Network Manager.

4.2.3.6
Connection Groups Configuration

Connection Groups allow you to connect to multiple devices simultaneously. After connecting to multiple devices in a group, it is necessary to select which specific device (XRC or XRI) you wish to monitor or configure. When you want to monitor or configure a different device, you will need to select the new device. This will automatically de-select the previous site. The process of switching between selected devices can be done quickly when they are part of the same Connection Group because the connections have already been established.

The Connection Groups tab is used to create Connection Groups. Only TCP/IP connections are eligible to be placed into a Connection Group. The Connection Groups Tab is also used to name the Group, save the Group, edit or delete Connection Groups, and to launch a connection to the desired group.

Figure 28: Connection Groups Settings Screen



Select a group or create a new one below

Connection Group Name: NID 250 Primary Controllers Group

TCP/IP Connections

Connection Name	IP Address
NID 250 - Site 001 -...	172.25.1.200
NID 250 - Site 002 -...	172.25.2.200
NID 250 - Site 003 -...	172.25.3.200
NID 250 - Site 004	172.25.4.200
NID 250 - Site	25.5.200
NID 250 - Site	25.71.100
NID 250 - Site 07	25.72.100
NID 250 - Site 073 -...	172.25.73.100
NID 250 - Site 074 -...	172.25.74.100
NID 250 - Site 075 -...	172.25.75.100
NID 250 - Site 076 -...	172.25.76.100
NID 250 - Site 077 -...	172.25.77.100
NID 250 - Site 078 -...	172.25.78.100

Total TCP/IP Connections:72

Connection Group

Connection Na...	IP Address	Port
NID 250 - Site 0...	172.25.1.100	4444
NID 250 - Site 0...	172.25.2.100	4444
NID 250 - Site 0...	172.25.3.100	4444
NID 250 - Site 0...	172.25.4.100	4444
NID 250 - Site 0...	172.25.5.100	4444

Total Connections: 5

1 Connection Groups Dropdown. Click here to view/select from existing connection groups.

2 Available Site Connections. (these are added/configured using the Connections tab)

3 Sites added to the Connection Group.

4 Add/Remove arrows. Click the right-facing arrow to add a selected connection to the group. Click the left-facing arrow to remove a selected connection from the group.

5 Launch Network Manager. Make Connection with Controllers in Connection Group.

4.2.3.6.1 Creating and Saving a Connection Group

Prerequisites:

- Devices in a connection group must all be part of the same Network (must share the same Network ID). The Connection Tool does not enforce this rule when creating the Connection Group, but it does enforce the rule when establishing connections with XRC sites.
- This recommendation pertains to creating a Connection Group that contains all network sites: If a site has both Primary and Secondary controllers, do not place connections for both the Primary and Secondary in the Connection Group. Use only the connection with the Primary Controller IP address. There is no need to add a secondary controller to the connection group. The tool automatically connects to whichever controller is controlling the site at the time. Including both connections in the same group can create confusion (and possibly result in configuring the wrong XRC). If you need to connect with the inactive controller (that is, the one not currently controlling the site), you should launch an individual connection to the Secondary Controller IP address from the “Connections” tab.
- You may create a connection group containing just one connection, but there is no advantage to doing so.

Procedure:

1. Select one or more connections from the list of available connections on the left and click the right facing arrow button to add the connection(s) to the Connection Group in the right-hand column.
2. Enter a name for the connection group.
3. Click the **Save** button.

4.2.3.6.2 Editing an Existing Connection Group

Prerequisites: To edit an existing connection group, select it from the dropdown list on the Connection Groups tab and make the desired changes.

Procedure:

1. Select the Connection Group from the drop down box at the top of the Connection Groups tab.
2. Make the desired changes.
3. Click the **Save** button.

4.2.3.6.3 Deleting a Connection Group

Procedure:

1. Select the group to delete from the drop down box at the top of the Connection Groups tab.
2. Click the **Delete** button.
3. Group is deleted.

   The connections that make up the group are not deleted

4.2.3.6.4
Connecting to Multiple Sites Using a Connection Group

Procedure:

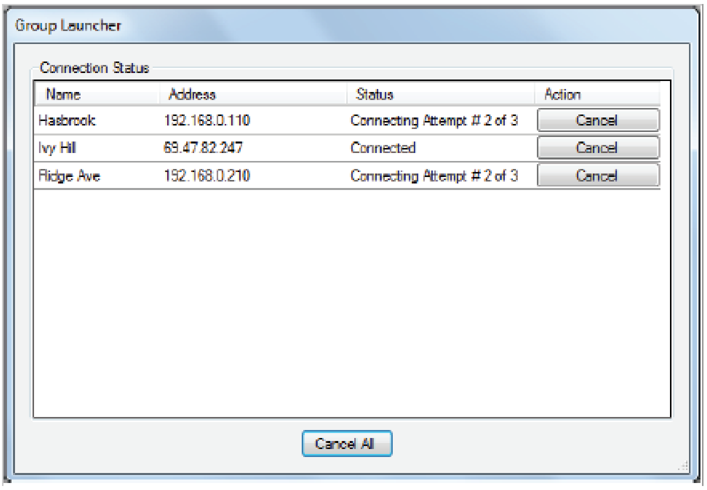
1. Start the Network Manager Connection Tool.
2. Click on the Connection Groups tab.
3. Select the group you want to connect to from drop down box at the top of the Connection Groups tab (or create a new group).
4. Click the **Launch Network Manager** button.

   The Login screen appears.
5. Enter the Username and Password, and then click **Login**.

   Each device in the Connection Group must have an account with the entered Username and Password. See User Roles on page 157for information on how to set up login accounts.

   A Connection Status window appears.

   Figure 29: Group Launcher Screen

   Group Launcher

   Connection Status

Name	Address	Status	Action
Hasbrook	192.168.0.110	Connecting Attempt # 2 of 3	Cancel
Ivy Hill	69.47.82.247	Connected	Cancel
Ridge Ave	192.168.0.210	Connecting Attempt # 2 of 3	Cancel

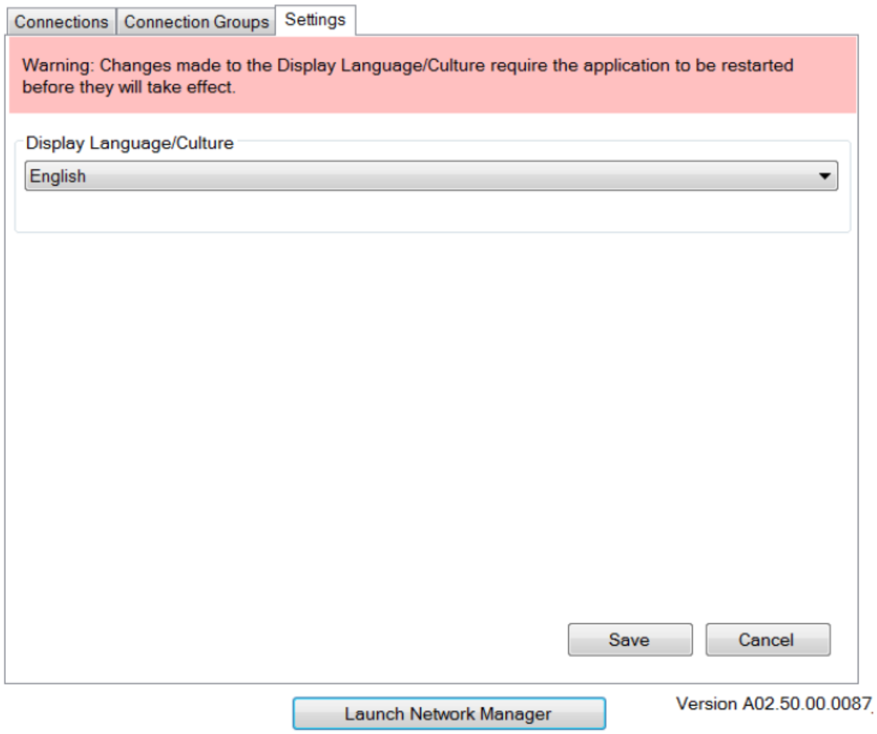
6. During the establishment of connections to the group, the Group Launcher window displays the Connection Status.
   - To cancel a specific connection, click the **Cancel** button to the right of the Status column.
   - To cancel all connections to this group, click **Cancel All**.

A maximum of three (3) attempts per controller are made. Once the connections and attempts are complete, the window disappears and the Network Manager opens with the Site Dashboard displayed. Any connection that could not be established in three attempts will display with gray box in the Site Dashboard.

4.2.4 Settings Configuration

This Settings tab allows you to configure display language/culture.

Figure 30: Network Connection Tools Settings Tab



Warning: Changes made to the Display Language/Culture require the application to be restarted before they will take effect.

Display Language/Culture: English

Version A02.50.00.0087

4.2.4.1 Selecting the Network Manager Connection Tool Language

The application can be configured to display in English, or in the same language as the operating system of the computer (if other than English and supported by the application).

Procedure:

1. Click the **Settings** Tab.
2. Click the arrow under **Display Language/Culture**.

   The application displays a list of one or two languages.
3. Select the desired Language/Culture from the list and press **Save**.
4. Manually close, then restart the application to enforce the language change immediately.

   NOTICE: The language change is automatically communicated to the Network Manager application the next time it is launched by the Network Manager Connection Tool.

Postrequisites: Changes to the Display Language/Culture require the application to be manually restarted before the changes take effect.

4.2.5 Site Dashboard

When the Connection Tool has established connections to all available sites, and has downloaded the most recent available copy of the Network Manager (if the PC does not already have the same copy – or a more recent copy), the Network Manager program launches and displays the **Site Dashboard** in the **Details View**.

The Site Dashboard supports two views: The **Details View** and the **Icon View**. The **Details View** is the default view when the Network Manager launches. There are two ways to switch between the two views. See Switching Between Details and Icon View on page 74 for more info.

The **Site Dashboard** has three major functions:

- It shows which device connections were and were not successful. If the Connection Tool was not able to establish a successful connection after three attempts, the box representing the site displays with gray highlighting in the Site Dashboard.
- For successfully connected controllers, the **Site Dashboard** shows whether or not there are any active Controller Alerts or Repeater Alarms.
- The **Site Dashboard** makes it possible to select a specific device for the purposes of configuring the controller or obtaining more information about the device.

The **Site Dashboard** allows you to quickly choose a controller to view/configure. Colors are used to quickly identify site status:

Blue highlighted text
Currently Selected Device.

Red box
Site with an active Controller Alert or Repeater Alarm, but not the Selected site.

White box
Connected to an XRC, but not the Selected device.

Light Blue box
Connected to an XRI Interconnect Gateway, but not the Selected device.

Gray box
`Not Connected` Device.

Reasons why a device might show as `Not Connected` include the following scenarios:

- Failure to connect in three attempts.
- Not able to authenticate with the device using the entered Username and Password combination
- The Network ID of the device was different than the Network ID of the first successfully connected device.

It is also possible for a device to initially show as connected, and then later show as disconnected. This will occur if the TCP/IP connection was initially good, but was later lost. This can occur due to a network connectivity issue, or because the device rebooted.

For each successful XRC connection, the controller's configured role (Stand-alone, Primary, Secondary) is displayed in the column called Role/State in the **Details View**.

- The device state shows `Active` if that controller is currently in control of the site (for example, Primary / Active).
- The device state shows `Inactive` if the controller is not currently in control of the site.

IMPORTANT: As a general rule, do not make configuration changes to an XRC if the word `Inactive` appears on the row at the bottom of the box representing the connection. This indicates that you have connected to the inactive controller in a redundant pair. Changes to this XRC would likely be overwritten or lost. For more information, see the "Redundant Controller" section of the *MOTOTRBO Connect Plus System Planner*.

To select a device to view/edit, click on the row corresponding to the device (**Details View**) or the box corresponding to the device (**Icon View**). The currently selected row or box is highlighted in Blue, and (for a XRC site) you can see the IP address, port number, Site Number and Network ID for the currently connected device at the bottom of the Network Manager window. The Network Manager does not allow you to switch the selected device while there are windows open for the currently selected site. If you attempt to select a different device prior to closing any open windows for your current site, you will receive a prompt, reminding you that there are open windows.

- If you click **Yes**, the Network Manager will close the open windows and switch to the new device.
- If you click **No** or **Cancel**, the Network Manager will leave the windows open (and you will remain connected to the current device).

4.2.5.1 Switching Between Details and Icon View

Procedure:

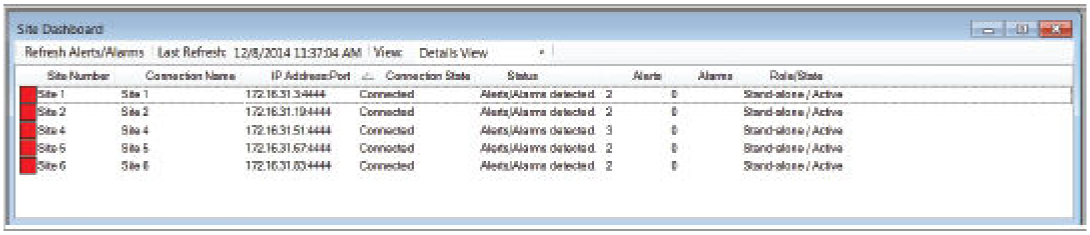
Perform one of the following actions:

- Click the box labeled **View:** at the top of the **Site Dashboard** window, then select the desired view from the drop-down list.
- Right click within the **Site Dashboard** and select either **View** → **Details View** or **View** → **Icon View** from the pop-up menu options.

4.2.5.2 Site Dashboard in Details View

The **Details View** displays as a grid with rows and columns. Each row represents a device connection.

Figure 31: Site Dashboard in Details View



Site Dashboard

Refresh Alerts/Alarms | Last Refresh: 12/8/2014 11:37:04 AM | View: Details View

Site Number	Connection Name	IP Address:Port	Connection State	Status	Alerts	Alarms	Role/State
🟥 Site 1	Site 1	172.16.31.3:4444	Connected	Alerts/Alarms detected	2	0	Stand-alone / Active
🟥 Site 2	Site 2	172.16.31.19:4444	Connected	Alerts/Alarms detected	2	0	Stand-alone / Active
🟥 Site 4	Site 4	172.16.31.51:4444	Connected	Alerts/Alarms detected	3	0	Stand-alone / Active
🟥 Site 5	Site 5	172.16.31.67:4444	Connected	Alerts/Alarms detected	2	0	Stand-alone / Active
🟥 Site 6	Site 6	172.16.31.83:4444	Connected	Alerts/Alarms detected	2	0	Stand-alone / Active

Column Name	Details
Site Number	Box icon to represent the connection. The color of the box conveys information about the connection. After the icon, the Network Manager displays the Site Number (for connected XRC devices), `XRC` for Disconnected XRC Controllers, or `XRI` for a Connected or Disconnected XRI Interconnect Gateway.
Connection Name	The Connection Name as configured in the Network Manager Connection Tool.
IP Address and Port	The IP Address and Port that the Network Manager uses to communicate with the device.

Column Name	Details
Connection State	**Connected** The Network Manager is connected to the device. **Connecting** The Network Manager is attempting to connect to the device. **Disconnected** The Network Manager is not connected to the device. **Rebooting** The Network Manager cannot connect because device reboot is imminent.
Status	**Alerts/Alarms detected** The connected device has reported one or more Alerts or Alarms. **Blank** The Network Manager is attempting to connect to the device. **Connected** The Network Manager is connected to the device, and no Alerts or Alarms have been reported. **Disconnected** The Network Manager is not connected to the device. **Site Alerts/Alarms failed to download** There was problem downloading Alerts/Alarms from the device.
Alerts	Shows the number of Controller Alerts reported by the device. `N/A` is displayed for XRI Gateways and Disconnected XRC Controllers.
Alarms	Shows the number of Repeater Alarms reported by the device. `N/A` is displayed for XRI Gateways and Disconnected XRC Controllers.
Role/State	The word to the left of the slash indicates the device’s role. The word to the right of the slash indicates the device’s current state. For Disconnected Devices, this column is blank. For Connected Devices: **Roles** Stand-alone, Primary, or Secondary, depending on the Controller Role as configured with the Network Manager. A connected XRI Gateway displays as `Stand-alone`. **States** `Active` or `Inactive`. For XRC Controllers, `Active` indicates the device is in control of the site. `Inactive` indicates the device is not in control of the site. A connected XRI Gateway displays as `Active`.

4.2.5.2.1 Using the Details View

When and where to use: The following adjustments can be done to in the **Details View**.

Procedure:

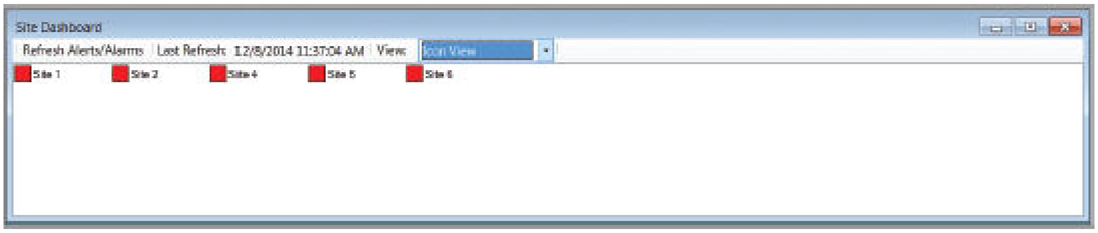
- Adjust the width of the columns in the Details View by dragging the lines that separate the column headings to the left or right.
- Sort the information in **Details View** by clicking on the column heading which will be used as search criteria to perform an alphanumeric sort (or a reverse alphanumeric sort, depending on how the information is displayed to begin with).

  Following the sort, the up or down arrow shows how the information is sorted. An up arrow indicates the information is sorted 0-9, A-Z. A down arrow indicates the information is sorted 9-0, Z-A.

4.2.5.3 Site Dashboard in Icon View

The **Icon View** contains an icon (a square box) for each attempted connection and some brief text to describe the connection or device. The **Icon View** contains no other information, but is useful for representing a large number of device connections within the **Site Dashboard** window.

Figure 32: Site Dashboard in Icon View



Last Refresh: 12/8/2014 11:37:04 AM

View: Icon View

4.2.5.4 Alarm Display in Site Dashboard

Sites with active Controller Alerts and/or Repeater Alarms are shown with a red box icon. In the Details View, the number of active Controller Alerts and Repeater Alarms for each connected site are shown in the columns called “Alerts” and “Alarms”. If there are no active Controller Alerts or Repeater Alarms, the Network Manager displays the number 0 (zero) in the corresponding column(s). If the row represents an Inactive XRC Controller, or an XRI, or a Disconnected device, then the Network Manager displays N/A in both the Alert and Alarm Columns.

Alerts/Alarm data may be manually refreshed by pressing the **Refresh Alerts/Alarms** button. The data does not automatically refresh.

The information on the Site Dashboard tells you when a site has one or more active Alert(s) and/or Alarm(s), but it does not provide any details. For that information, it will be necessary to select a site and open the Alerts/Alarms Management screen as described in the "Alerts/Alarms Management Window" Section.

4.2.5.5 Disconnection and Connection via the Right-Click Menu

This feature allows the user to disconnect from a specific device (without closing the Network Manager), or to connect/re-connect to a specific device, via a right-click option from the **Site Dashboard**.

This feature is supported with the following constraints:

- The feature is available for TCP/IP Connections only. It is not available for modem connections.
- It is not possible to change user roles for a subsequent connection via this method. To change user roles, it will be necessary to first close down the Network Manager (by selecting **Disconnect** from the Menu bar), and then to re-launch the Network Manager Connection Tool.
- Reconnection via the right-click menu is not allowed following a site firmware upgrade. To re-connect following a site firmware upgrade, it will be necessary to first close down the Network Manager (by selecting **Disconnect** from the Menu bar), and then to re-launch the Network Manager Connection Tool.

4.2.5.5.1 Disconnecting via the Right-Click Menu

Procedure:

To disconnect from a specific device (without disconnecting from all sites or closing the Network Manager), position the pointer over the row or icon that corresponds to the desired device, right-click, and select **Disconnect** from the pop-up menu.

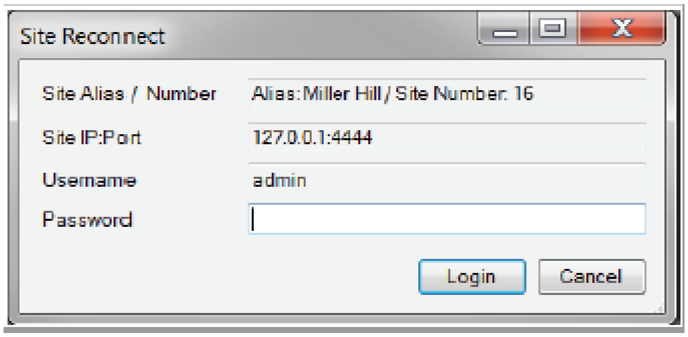
4.2.5.5.2 Connecting (or Re-connecting) via the Right-Click Menu

Procedure:

1 If a device did not connect on the initial attempt, or the device disconnected following the initial connection, attempt to reconnect as follows, position the pointer over the row or icon that corresponds to the desired device, right-click, and select **Connect** from the pop-up menu.

The **Site Reconnect** window appears.

Figure 33: Site Reconnect Window



Site Reconnect

Site Alias / Number	Alias: Miller Hill / Site Number: 16
Site IP:Port	127.0.0.1:4444
Username	admin
Password	

2 Review the connection details (Site Alias, Site Number, Site IP address: Network Manager TCP Port, and Username), enter the Password, and click **Login** (or **Cancel**).

The Network Manager will then attempt to connect to the site. The icon or row that represents the site on the Site Dashboard will show whether the connection attempt is successful.

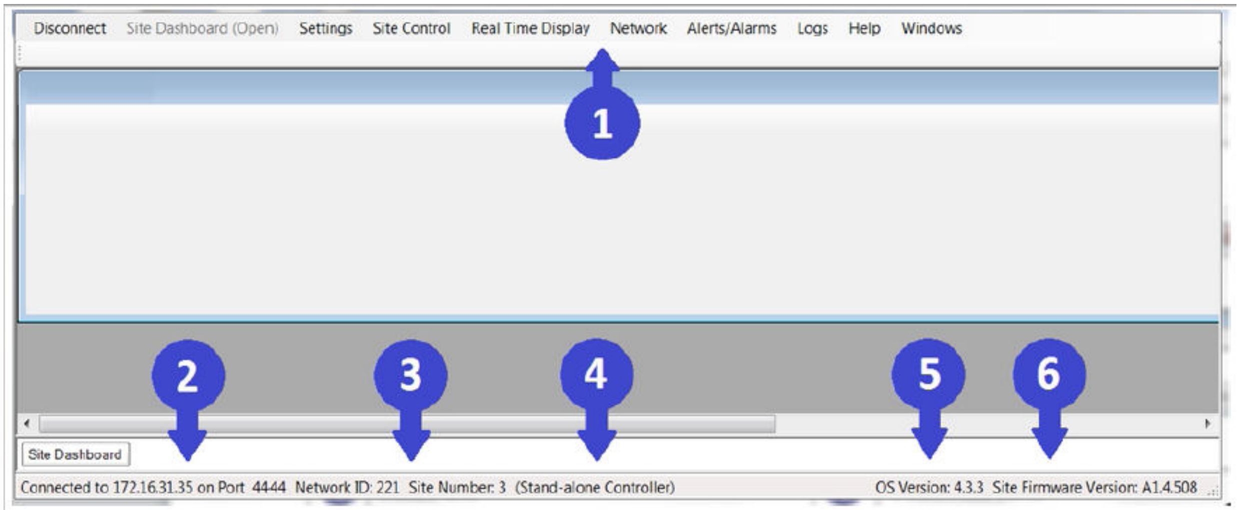
NOTICE: Depending on why the device failed to connect (or why the device disconnected), the **Connect** option may not be available via the right-click menu. When this occurs, close the Network Manager (by selecting **Disconnect** from the Menu bar), and then re-launch the Network Manager Connection Tool.

Chapter 5

Site and Network Configuration

5.1 XRC Configuration Screen

Figure 34: XRC Configuration Screen



Connected to 172.16.31.35 on Port 4444 Network ID: 221 Site Number: 3 (Stand-alone Controller) OS Version: 4.3.3 Site Firmware Version: A1.4.508

1 Menu Bar

2 Currently connected to this IP address and port

3 Network ID & Site Number of currently Selected XRC (and a connection is present)

4 Controller Role

5 OS Version

6 Site Firmware Version

5.1.1 Critical Settings Configuration

The device has two types of configurable settings: Critical and Non-Critical.

- Critical Settings require a device reboot to take effect.
- Non-Critical settings do not require a device reboot to take effect.

If the application user attempts to save a critical setting, the application provides a warning message as shown in the following image. The message provides two options: **Reboot Now** and **Reboot Later**.

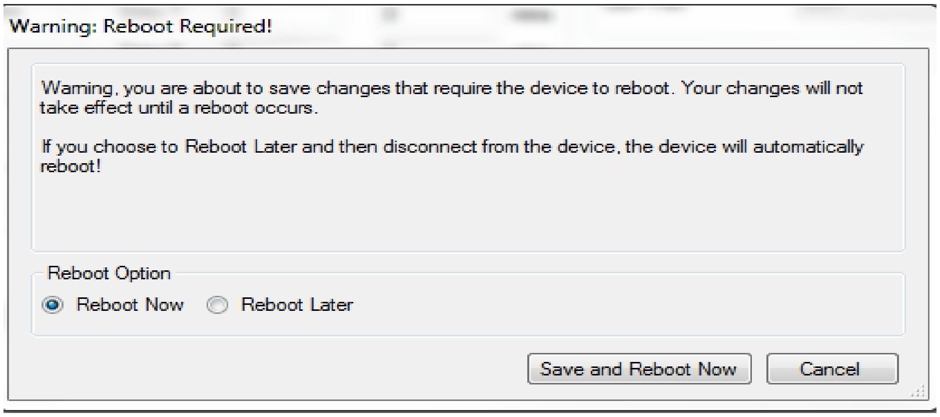
Reboot Now
Reboots the device immediately. The changes take effect when reboot is complete.

Reboot Later
Buffers the changes and defers the reboot to a later time. The changes do not take effect until the reboot occurs (and is completed).

Reboot Warning
During reboot, the device is not operational until the reset completes and the device users reconnect and/or re-register. The time required for reboot varies from a couple of minutes to several

minutes, depending on what is being updated. In the meantime, device users may experience an interruption of service.

Figure 35: Reboot Warning Prompt



Warning: Reboot Required!

Warning, you are about to save changes that require the device to reboot. Your changes will not take effect until a reboot occurs.

If you choose to Reboot Later and then disconnect from the device, the device will automatically reboot!

Reboot Option

● Reboot Now ○ Reboot Later

5.1.1.1

Rebooting the Device Now

Procedure:

1 Under **Reboot Option**, select **Reboot Now**.

2 Click **Save and Reboot Now**.

When the device accepts the reboot request, the application displays a Reboot Status message saying the device must complete current processing operations before the reboot begins. The message closes when the application disconnects due to the reboot, or the application user can click **Disconnect Now** to immediately close the message and disconnect from the device.

Postrequisites: Manually reconnect after the reboot is complete.

5.1.1.2

Rebooting the Device Later

Procedure:

1 Under **Reboot Option**, select **Reboot Later**.

2 Press the **Save and Reboot Later** button.

The screen closes, and the application remains connected to the device.

Postrequisites: Reboot the device for changes to take effect. The reboot occurs when the device disconnects from the application. The disconnect can be either a voluntary disconnect triggered by the application user or involuntary disconnect due to a connectivity, hardware, or software issue. Examples of voluntary disconnects include selecting the **Reboot** option, selecting the **Disconnect** option, closing the application, and so on.

5.1.1.3

Indications of Pending Reboot

If the application user selects **Reboot Later**, the device enters Pending Reboot state, and it remains in this state until the device reboots.

The application provides several indications of Pending Reboot state on a connected device. The exact indications differ depending on the following situations:

- The application session made the critical change(s) and the user opted to Reboot Later.
- A different application session is connected to the same device.

NOTICE: It is recommended that multiple sessions (or instances) of the application should **not** be simultaneously connected to the same device.

All sessions of the application display the words `Pending Reboot` after the device role in the **Status** bar at the bottom of the screen.

The application session that made the critical change(s) and opted to Reboot Later displays a pink banner underneath the main menu. A warning message advises that one or more connected devices are in Pending Reboot state, and that disconnecting from the devices will cause the device(s) to immediately reboot.

While in Pending Reboot state, the application session that made the critical change(s) and opted to Reboot Later is allowed to make subsequent edits to device settings prior to the Reboot. However, if a different application session is also connected to the device, the application displays a message advising that the device is in Pending Reboot state due to changes made by a different application session, and that changes cannot be made until the device reboots.

5.1.2
Configuring Network Settings

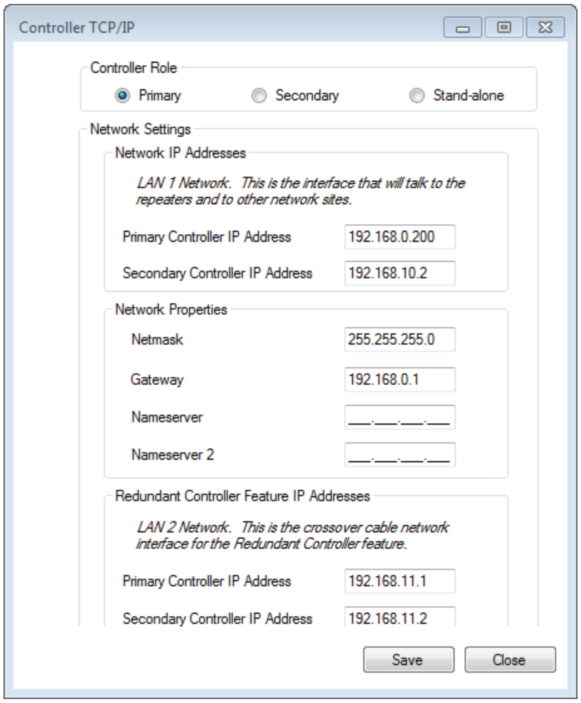
Procedure:

1 Click on **Network** in the Menu bar.

2 Select **Settings** from the dropdown menu.

The Network Configuration window appears.

Figure 36: Controller Role and Network Settings Screen



Controller TCP/IP

Controller Role

● Primary ○ Secondary ○ Stand-alone

Network Settings

Network IP Addresses

LAN 1 Network. This is the interface that will talk to the repeaters and to other network sites.

Primary Controller IP Address 192.168.0.200

Secondary Controller IP Address 192.168.10.2

Network Properties

Netmask 255.255.255.0

Gateway 192.168.0.1

Nameserver ___.___.___.___

Nameserver 2 ___.___.___.___

Redundant Controller Feature IP Addresses

LAN 2 Network. This is the crossover cable network interface for the Redundant Controller feature.

Primary Controller IP Address 192.168.11.1

Secondary Controller IP Address 192.168.11.2

5.1.2.1

Controller Role and Network Settings

Each Connect Plus site requires at least one controller. Beginning with Connect Plus Release 1.1, the customer can purchase a second controller per site to serve as backup to the primary controller. The secondary controller provides backup capability, but does not increase the number of repeaters and calls that can be managed per site.

The Network Configuration screen must be configured for every controller, regardless of whether the controller is a "stand-alone" (the only controller at the site), or is part of a Redundant Controller configuration. If the site employs a Redundant Controller configuration, read the "Redundant Controller" section of the *MOTOTRBO Connect Plus System Planner* prior to configuring this screen. The System Planner contains diagrams illustrating connections, important operational information, and steps to be followed when configuring and deploying Redundant Controllers at the site.

NOTICE: The controller must reboot to save changes to the Network Configuration.

5.1.2.1.1

Setting the Controller Role

Prerequisites: In a redundant controller configuration, the Network Configuration screen must be configured into each controller (these settings do not transfer when doing a “Backup and Restore” operation). Except for Controller Role, the screen must be configured with identical information in both the Primary and Secondary controller. It is also important to note the Redundant Controller setup requires four different, static IP addresses. See the *MOTOTRBO Connect Plus System Planner* for important information on configuring and deploying redundant XRC controllers.

Procedure:

Select one of the following radio buttons:

Primary
When the site has two XRC controllers in a redundant configuration, select this bullet when configuring the Primary controller. This is the controller that will be in control of the site during normal operation.

Secondary
When the site has two XRC controllers in a redundant configuration, select this bullet when configuring the Secondary controller. This is the controller that will be on standby in normal operation.

Stand-alone
Select when there is only one XRC for this site (default setting).

5.1.2.2

Network Settings: LAN 1 Network

The LAN 1 Network is comprised of the devices that are connected to the site LAN Ethernet switch. This is the network used for all communications with the site's clients, and with other Connect Plus sites. If this site does not have redundant devices, then LAN 1 is the only network. The device is connected to the LAN 1 network by way of the port labeled "LAN1" on the back of the device .

NOTICE: In redundant operation, the Primary and Secondary devices have the ability to automatically swap their LAN 1 IP addresses in the background, but this does not change how the Network Manager displays the LAN 1 IP addresses. The Network Manager always displays the LAN 1 addresses as configured with this screen.

5.1.2.2.1

Entering the Primary Controller IP Address

Procedure:

1. Enter the IP address of Primary Controller on its LAN 1 network.

   This field is also used for the IP address of a stand-alone controller. The format and range for the address are (000-255).(000-255).(000-255).(000-255).

2. Enter the Primary or stand-alone IP address assigned by your IT manager.

   NOTICE: The combination of the Primary (or Secondary) IP Address configured on the TCP/IP screen and the TCP Control Port (**Settings** → **Configuration**) cannot be the same as any Global IP Address and Global TCP Port combination configured on the MultiSite Configuration screen (**Settings** → **MultiSite**).

5.1.2.2.2

Entering the Secondary IP Address

Procedure:

1. Enter the IP address of the secondary device (if so equipped) on its LAN 1 network.

   If this site does not have a redundant device, this field is left blank. The format and range for the address are ***<000-255>.<000-255>.<000-255>.<000-255>***.

2. Enter the secondary IP address assigned by your IT manager.

5.1.2.2.3

Entering the Netmask

Procedure:

Enter the subnet mask (IP Mask or Netmask) assigned by the IT manager.

The format and range for the address are ***<000-255>.<000-255>.<000-255>.<000-255>***.

5.1.2.2.4

Entering the Gateway (Router) IP Address

Procedure:

In the Gateway field, enter the Gateway IP address assigned by your IT manager.

This IP address belongs to the network node that is responsible for routing messages to and from this Local Area Network. The format and range for the address are ***<000-255>.<000-255>.<000-255>.<000-255>***.

5.1.2.2.5

Entering the Domain Name Server(s)

Procedure:

Enter the IP Address of the preferred Domain Name Server (DNS) as assigned by the IT Manager.

The format and range for the address are ***<000-255>.<000-255>.<000-255>.<000-255>***. Use of this parameter is optional.

5.1.2.3
Network Settings: LAN 2 Network

The LAN 2 Network fields are only used if the site has two devices, in redundant configuration. The LAN 2 network is a private network consisting only of the primary and secondary devices, which must be directly connected from the port labeled "LAN2" on the primary device to the port labeled "LAN2" on the secondary device. An Ethernet crossover cable is recommended for the direct connection. When configuring a redundant pair of devices, the LAN 2 configuration is critical.

5.1.2.3.1
Entering the Primary Controller IP Address

Procedure:

1. Enter the IP address of Primary Controller on its LAN 2 network.

   The first three octets of this IP address must match the Secondary Controller (LAN 2) IP address exactly. The first three octets of this address must be different than the first three octets of Primary and Secondary Controller IP Addresses for the LAN1 Network. The format and range for the address are (000-255).(000-255).(000-255).(000-255).
2. Enter the Primary LAN 2 IP address assigned by your IT manager.

5.1.2.3.2
Entering the Secondary IP Address

Procedure:

1. Enter the IP address of the secondary device on its LAN 2 network.

   The first three octets of this IP address must match the primary device (LAN 2) IP address exactly. The first three octets of this address must be different than the first three octets of primary and secondary devices' IP Addresses for the LAN 1 Network. The format and range for the address are (000-255).(000-255).(000-255).(000-255).
2. Enter the secondary LAN 2 IP address assigned by your IT manager.

5.1.3
Configuring Site Settings

Procedure:

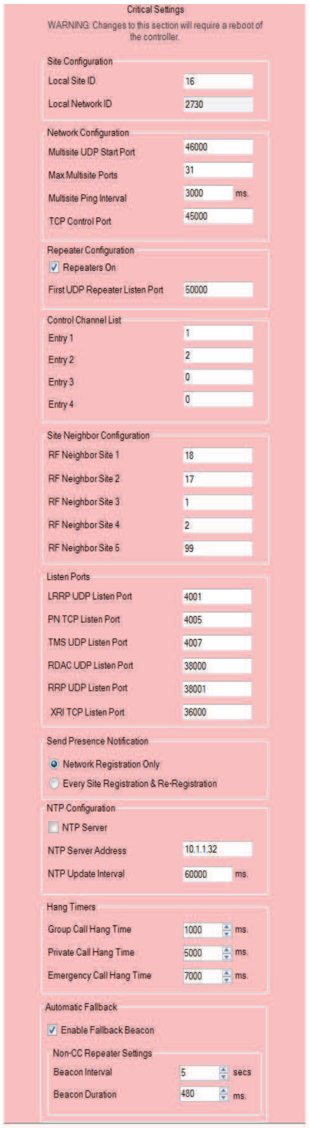
1. Click on **Settings** in the Menu Bar.
2. Click on **Configuration** in the menu.
3. Click on the **Configuration Tab** (if not already selected).

   The Site Configuration screen appears.

5.1.3.1
Site Settings - Critical

⚠ **CAUTION:** Changes to this section require a reboot of the device.

Figure 37: Critical Settings Screen



Critical Settings

WARNING: Changes to this section will require a reboot of the controller.

Site Configuration

Local Site ID: 16

Local Network ID: 2730

Network Configuration

Multisite UDP Start Port: 46000

Max Multisite Ports: 31

Multisite Ping Interval: 3000 ms.

TCP Control Port: 45000

Repeater Configuration

☑ Repeaters On

First UDP Repeater Listen Port: 50000

Control Channel List

Entry 1: 1

Entry 2: 2

Entry 3: 0

Entry 4: 0

Site Neighbor Configuration

RF Neighbor Site 1: 18

RF Neighbor Site 2: 17

RF Neighbor Site 3: 1

RF Neighbor Site 4: 2

RF Neighbor Site 5: 99

Listen Ports

LRRP UDP Listen Port: 4001

PN TCP Listen Port: 4005

TMS UDP Listen Port: 4007

RDAC UDP Listen Port: 38000

RRP UDP Listen Port: 38001

XRI TCP Listen Port: 36000

Send Presence Notification

● Network Registration Only

○ Every Site Registration & Re-Registration

NTP Configuration

□ NTP Server

NTP Server Address: 10.1.1.32

NTP Update Interval: 60000 ms.

Hang Timers

Group Call Hang Time: 1000 ms.

Private Call Hang Time: 5000 ms.

Emergency Call Hang Time: 7000 ms.

Automatic Fallback

☑ Enable Fallback Beacon

Non-CC Repeater Settings

Beacon Interval: 5 secs

Beacon Duration: 480 ms.

5.1.3.1.1
Site Configuration Parameters

5.1.3.1.1.1
Local Site ID

This is the site number of the device.

Minimum	1
Maximum	250
Increment	1
Default	1

5.1.3.1.1.2 *Local Network ID*

This parameter describes the Network ID transmitted over-the-air by the device. The Network ID must be the same across the whole network, and must match the Network ID programmed into Connect Plus radios using the network.

NOTICE: This parameter is set in the factory and cannot be changed.

5.1.3.1.2 Network Configuration Parameters

The following topics describe the information which needs to be filled in each Network Configuration field.

5.1.3.1.2.1 *Multisite UDP Start Port*

The device listens to a range of UDP ports for incoming voice packets. This parameter defines the first UDP port in the range.

Minimum	4000
Maximum	65503
Increment	1
Default	46000

5.1.3.1.2.2 *Max Multisite Ports*

Defines the range of UDP port numbers device will listen to for incoming voice packets. For example, if Multisite UDP Start Port is 46,000, and if Max Multisite Ports is 32 (recommended value), device will listen for incoming voice packets on ports 46,000-46,031).

Minimum	1
Maximum	32
Increment	1
Default	32

5.1.3.1.2.3 *Multisite Ping Int (ms)*

Defines the ping interval the device uses to verify the TCP/IP communications link with other network sites.

Minimum	2500
Maximum	10000
Increment	1
Default	2500

5.1.3.1.2.4 *TCP Control Port*

This parameter defines the port this device uses for receiving TCP control messages from other network sites.

Minimum	4000
Maximum	65535
Increment	1
Default	45000

5.1.3.1.3 Repeater Configuration Parameters

The sections which follow explain how each field in the Repeater Configuration parameters are to be completed.

5.1.3.1.3.1 *Repeater On*

When this check box is checked, the device attempts to assign calls to any repeater that has checked in with it.

When this check box is unchecked, the device does not attempt to assign calls to any repeater.

5.1.3.1.3.2 *First UDP Repeater Listen Port*

The device listens to a range of 15 ports for MOTOTRBO repeaters. This parameter explicitly defines the first port in the range, and implicitly defines the other 14 ports as well.

Example: If the First UDP Repeater Listen Port value is 51,000, the device listens for repeaters on 51,000 through 51,014.

Minimum	4000
Maximum	65520
Increment	1
Default	51000

5.1.3.1.3.3 *Control Channel List*

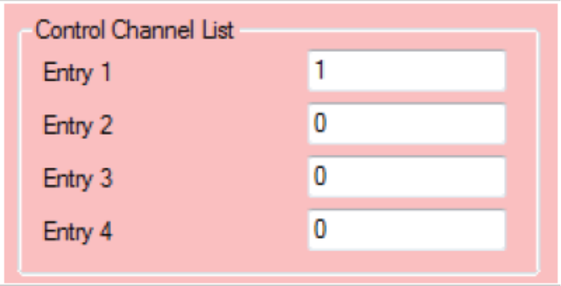
Up to four (4) repeaters at a site may be designated as potential Control Channel (CC) repeaters. Only one repeater at a time will be active as the current Control Channel. The Real Time Display shows which repeater has been most recently assigned as Control Channel.

- If a repeater is the active Control Channel repeater, timeslot 1 is used for control messages and timeslot 2 is used for call assignments.
- If a repeater is on the Control Channel List, but is not the active Control Channel, both timeslots will be used for call assignment.

The Control Channel can "Failover" to one of the other repeaters on the list if the current CC repeater experiences a supported failure alarm. The Control Channel can also "Rollover" on a once-every-24-hours schedule to one of the listed repeaters. To be eligible for the Control Channel list, the repeater’s frequencies must be exclusively licensed. Shared, non-exclusive licenses are not suitable for Control

Channel operation. See Configuring Control Channel Rollover (Scheduled Rollover) on page 99 for more information. In addition, see the *MOTOTRBO Connect Plus System Planner* for a thorough discussion of Control Channel Failover and Rollover, including a list of the triggering events.

Figure 38: Control Channel List Entry Screen



Control Channel List

Entry 1	1
Entry 2	0
Entry 3	0
Entry 4	0

You may enter up to four (4) repeaters in this list (each site must have at least one Control Channel repeater defined). Enter the Radio ID (1-15) of each repeater to be used as Control Channel. If there are fewer than four entries, the Repeater Radio IDs should be entered from the top down. Use Entry 1 before Entry 2, and so forth. Zero (0) indicates the entry is unused. If the Network Manager connects to a device that is running firmware prior to Connect Plus Release 1.1, entries 2-4 are grayed out.

Minimum	0
Maximum	15
Increment	1
Default	1 for Entry 1, 0 for Entries 2-4

NOTICE: Prior to making any changes to this list with Network Manager, use MOTOTRBO Connect Plus CPS to update the Network Frequency File in the Connect Plus subscriber units so that it matches the Control Channel information to be configured in this list.

5.1.3.1.3.4 CC Repeater Radio ID

This parameter describes the Radio ID of the Control Channel Repeater.

Minimum	1
Maximum	15
Increment	1
Default	1

5.1.3.1.4 Site Neighbor Configuration Parameters

5.1.3.1.4.1 RF Neighbor Site 1

This parameter defines the site number of the first network site that is adjacent in RF coverage to this site (or 0 if there is no RF neighbor).

Minimum	0
Maximum	250

Increment	1
Default	0

5.1.3.1.4.2 RF Neighbor Site 2

This parameter defines the site number of the second network site that is adjacent in RF coverage to this site (or 0 if there is no RF neighbor).

Minimum	0
Maximum	250
Increment	1
Default	0

5.1.3.1.4.3 RF Neighbor Site 3

This parameter defines the site number of the third network site that is adjacent in RF coverage to this site (or 0 if there is no RF neighbor).

Minimum	0
Maximum	250
Increment	1
Default	0

5.1.3.1.4.4 RF Neighbor Site 4

This parameter defines the site number of the fourth network site that is adjacent in RF coverage to this site (or 0 if there is no RF neighbor).

Minimum	0
Maximum	250
Increment	1
Default	0

5.1.3.1.4.5 RF Neighbor Site 5

This parameter defines the site number of the fifth network site that is adjacent in RF coverage to this site (or 0 if there is no RF neighbor).

Minimum	0
Maximum	250
Increment	1
Default	0

5.1.3.1.5
Listen Port Parameters

5.1.3.1.5.1
LRRP UDP Listen Port

This parameter defines the UDP Port on which the device listens for incoming messages from a Location Tracking application. (LRRP stands for Location Request Response Protocol.)

Minimum	4000
Maximum	65535
Increment	1
Default	4001

5.1.3.1.5.2
PN TCP Listen Port

This parameter defines the TCP Port on which the device listens for incoming messages from a Watcher application subscribing to the Presence Notification service of the device. (PN stands for Presence Notifier.)

Minimum	4000
Maximum	65535
Increment	1
Default	4005

5.1.3.1.5.3
TMS UDP Listen Port

This parameter defines the UDP Port on which the device listens for incoming messages from a Text Messaging application. (TMS stands for Text Messaging Service.)

Minimum	4000
Maximum	65535
Increment	1
Default	4007

5.1.3.1.5.4
RDAC UDP Listen Port

This parameter defines the UDP Port on which the device listens for incoming messages from an RDAC application. (RDAC stands for Repeater Diagnostics and Control.)

Minimum	4000
Maximum	65535
Increment	1
Default	38000

5.1.3.1.5.5 RRP UDP Listen Port

Defines the port on which this controller will listen for Remote Repeater Programming requests from an authorized version of MOTOTRBO CPS. Remote Repeater Programming (also known as IP Repeater Programming) is a purchasable feature for MOTOTRBO CPS.

Range	4000-65535
Increment	1
Default	38001

5.1.3.1.5.6 XRI TCP Listen Port

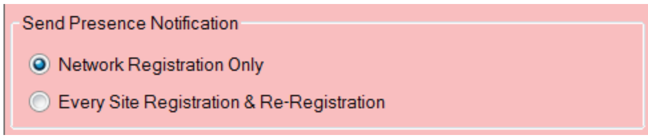
Defines the port on which this device will listen for connection from an XRI Interconnect Gateway.

Minimum	4000
Maximum	65535
Increment	1
Default	36000

5.1.3.1.6 Send Presence Notification

If this XRC Controller serves as Presence Notifier (PN) to a third-party "Watcher" application (supporting a third-party location tracking, text messaging or other application), the **Send Presence Notification** setting determines how often the XRC sends a NOTIFY message to indicate that a radio of interest is present.

Figure 39: Send Presence Notification Screen



Send Presence Notification

● Network Registration Only

○ Every Site Registration & Re-Registration

When configured for **Network Registration Only** (the default setting), this controller sends a NOTIFY Message indicating "present" when a radio that previously had not been registered with the network registers with any network site that has connectivity to this controller. As long as the radio remains registered to the network, the controller does not send NOTIFY Messages for subsequent registrations by the same radio due to changing sites, changing Talk Groups, returning from fade conditions (within the Controller’s configured **SU Inactivity Time**), and so on.

When configured for **Every Site Registration and Re-Registration**, the controller sends a NOTIFY Message indicating "present" when the radio sends any registration request (including re-registration) to any network site that has connectivity to this controller. A Connect Plus radio re-registers under many different circumstances – such as when the radio user changes the selected Talk Group, the radio roams to a different site, the radio returns from an extended fade condition, etc.

If this site does not serve as PN to a "Watcher" application, leave at the default setting. If this site serves as PN to a "Watcher" application, leave at the default setting unless directed otherwise by the vendor of the "Watcher" application software.

5.1.3.1.7 NTP Configuration Parameters

The XRC has an internal clock that tracks the date and time. The clock, which the controller utilizes for many important operations, uses Coordinated Universal Time (UTC). It is an international standard that correlates with time at the Royal Observatory in Greenwich, England.

In order to determine how this internal clock derives its time, the XRC must be configured as a Network Time Protocol (NTP) Server or as an NTP Client (that is, not an NTP Server).

- When configured as the NTP Server, the XRC keeps its own clock.
- When configured as the NTP Client, the XRC still keeps its own clock, but it periodically requests time updates from the NTP Server. The NTP Server Address and the NTP Update Interval are required settings for the client configuration. Upon receiving a response from the NTP Server, the controller adjusts its internal clock (if necessary) to align with the NTP Server. The clock should be initially set on the NTP Client by using the Network Manager's Date Time Configuration Screen as described in Date Time Configuration Section. Once the Client time is the same as the NTP Server (or at least within a few minutes of the server time), subsequent messages between the Server and Client keep the clocks in synch.

For single site systems, configure the XRC as NTP Server or NTP Client. When set as a client, the NTP Server Address (which will be some other network server – not an XRC) and the NTP Update Interval must be configured for the controller.

For multisite systems, all XRC controllers must derive their date and time from the same source. There are two acceptable configurations:

- One XRC can be set as NTP Server. All other XRC controllers must be configured as clients and point to the controller designated as the NTP Server.
- All XRC controllers can be configured as NTP Clients and point to the same NTP Server (which will be some other network server – not an XRC).

5.1.3.1.7.1 NTP Server

When this check box is checked, this site acts as a Network Time Protocol (NTP) Server. Other sites should be configured to point to this IP address of the site.

When this check box is unchecked, this site receives time updates from the NTP Server configured in the **NTP Server Address** field.

5.1.3.1.7.1.1 Entering the NTP Server Address

Procedure:

Enter the IP address or URL of the NTP Server, which can be the XRT, the XRC controller or a computer.

This field is grayed out if this device acts as the NTP Server.
The format for entering an IP address is *`<000-255>.<000-255>.<000-255>.<000-255>`*.

If entering a URL, the device must be configured with a valid Nameserver (reachable by this device) under **Network** → **Settings**.

5.1.3.1.7.2 NTP Update Interval

This parameter determines how often this device requests time updates from the NTP Server.

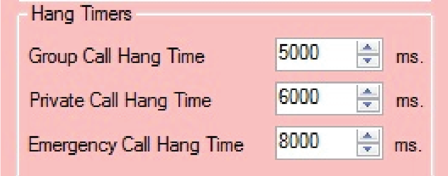
NOTICE: This field is grayed out if this device acts as the NTP Server.

Minimum	500 ms
Maximum	3600000 ms (1 hr)
Increment	1 ms
Default	60000 ms (1 min)

5.1.3.1.8

Hang Time Settings

Figure 40: Hang Timers Screen



Hang Timers

Group Call Hang Time 5000 ms.

Private Call Hang Time 6000 ms.

Emergency Call Hang Time 8000 ms.

Beginning with Connect Plus Release 1.1, the Group Call, Private Call and Emergency Call hang times are set using the Network Manager. The settings made here will be used to configure the repeaters directly when they first check in with the controller (thereby overwriting the Call Hang Time values configured with MOTOTRBO CPS). Whenever the transmitting radio in a call-in-progress releases the push to talk, the repeater starts the applicable call hang time timer. The call will stay up, and all resources will remain reserved. This is to allow the chance for another party to the call to reply. If the timer expires without any member of the call keying their radio, the call will be ended.

NOTICE: In earlier releases of the Connect Plus system, call hang times were set individually in each repeater using MOTOTRBO CPS. Repeaters must be at MOTOTRBO firmware release 1.8 or later to accept the hang time adjustment from the XRC. If the XRC fails to set the repeater Hang Time, it will create an Event Log entry stating this, along with the Radio ID of the repeater. When you see this Event Log entry, check the firmware version of the repeater. If the firmware version is prior to R01.08.00, upgrade the repeater firmware. If any network repeater has firmware prior to R01.08.00, then the Call Hang Times configured with the Network Manager must exactly match the Call Hang Times configured into the repeater via CPS (per call type).

IMPORTANT: When connecting to a XRC Controller running firmware prior to Connect Plus Release 1.1: If the Network Manager connects with a controller that is running Connect Plus firmware prior to Release 1.1, the labels on the three settings will be slightly different. Instead of being called Hang Timers, they will be called Inactivity Timers. This indicates that the Call Hang Time values should be set in the repeaters using MOTOTRBO CPS. In the Network Manager, set each Call Inactivity Timer to equal the corresponding Call Hang Timer set for the repeater, plus one second. For example, if Group Call Hang Time is set for 3 seconds with MOTOTRBO CPS, set the Group Call Inactivity Time to 4 seconds with Network Manager. It is important to note that Call Hang Timers should be set to the same value for every repeater and site in the network. For example, if Group Call Hang Time is 3 seconds and Private Call Hang Time is 4 seconds at Site 1, Repeater 1, then these same values should be set the same for every repeater network-wide.

IMPORTANT: Repeaters operating in Auto Fallback Mode: When a repeater is operating in Auto Fallback mode, it utilizes the Call Hang Time and SIT Timer values configured with MOTOTRBO CPS – not the Call Hang Time values configured with the Network Manager.

5.1.3.1.8.1
Group Call Hang Time

This setting configures the call hang time for Group Calls. For proper operation, the Group Call Hang Time must be set to the same value at all network sites.

Minimum	1000 ms
Maximum	7000 ms
Increment	500 ms
Default	3000 ms

5.1.3.1.8.2
Private Call Hang Time

This setting configures the call hang time for Private Calls. For proper operation, the Private Call Hang Time must be set to the same value at all network sites.

Minimum	2000 ms
Maximum	7000 ms
Increment	500 ms
Default	4000 ms

5.1.3.1.8.3
Emergency Call Hang Time

This setting configures the call hang time for Emergency Calls. For proper operation, the Emergency Call Hang Time must be set to the same value at all network sites. Note the maximum setting is 600000 ms (10 minutes).

Minimum	4000 ms
Maximum	600000 ms
Increment	500 ms
Default	4000 ms

5.1.3.1.9
Automatic Fallback

The Auto Fallback feature allows site repeaters to support limited radio operation (non-networked, non-trunked, Group Call communication) in certain site failure scenarios. The subscriber radio must be enabled for Auto Fallback operation with MOTOTRBO Connect Plus CPS and configured with the repeater and timeslot it will use for Auto Fallback at each network site. For a more complete discussion of Auto Fallback, see the *MOTOTRBO Connect Plus System Planner*.

5.1.3.1.9.1 Enabling Fallback Beacon

The Auto Fallback Beacon helps searching radios to know that the repeater is operating in Auto Fallback mode, and it tells radios already using the Fallback repeater not to roam away.

Procedure:

Check this box to enable Auto Fallback operation for the site repeaters.

When enabled, the site repeaters will transmit the Auto Fallback Beacon in certain site failure scenarios.

5.1.3.1.9.2 Non-CC Repeater Settings

The Non-CC Repeater Settings determine Auto Fallback operation for any site repeater that is not on the Control Channel List of the XRC.

5.1.3.1.9.2.1 Beacon Interval

When a non-Control Channel repeater is operating in Auto Fallback mode, this setting determines how often the repeater keys-up to transmit the Auto Fallback Beacon when there is no call taking place on either timeslot. A value of 0 seconds means that the repeater will transmit a continuous Fallback Beacon. The SU has a configurable setting in MOTOTRBO Connect Plus CPS called **Dwell Time for Non-Continuous Fallback Beacon**. It should be set to the same value as the Beacon Interval in the XRC. The one exception is when Beacon Interval is set to 0 seconds in the XRC. In that case, set the **Dwell Time for Non-Continuous Fallback Beacon** to 1 second in Connect Plus CPS programming.

Maximum	30 sec
Minimum	0 sec
Increment	1 sec
Default	5 sec

NOTICE: This setting is for Non-Control Channel repeaters only. It is not necessary to configure a Beacon Interval for repeaters that are on the Control Channel list of the XRC. Those repeaters always send a continuous Beacon in Auto Fallback mode.

5.1.3.1.9.2.2 Beacon Duration

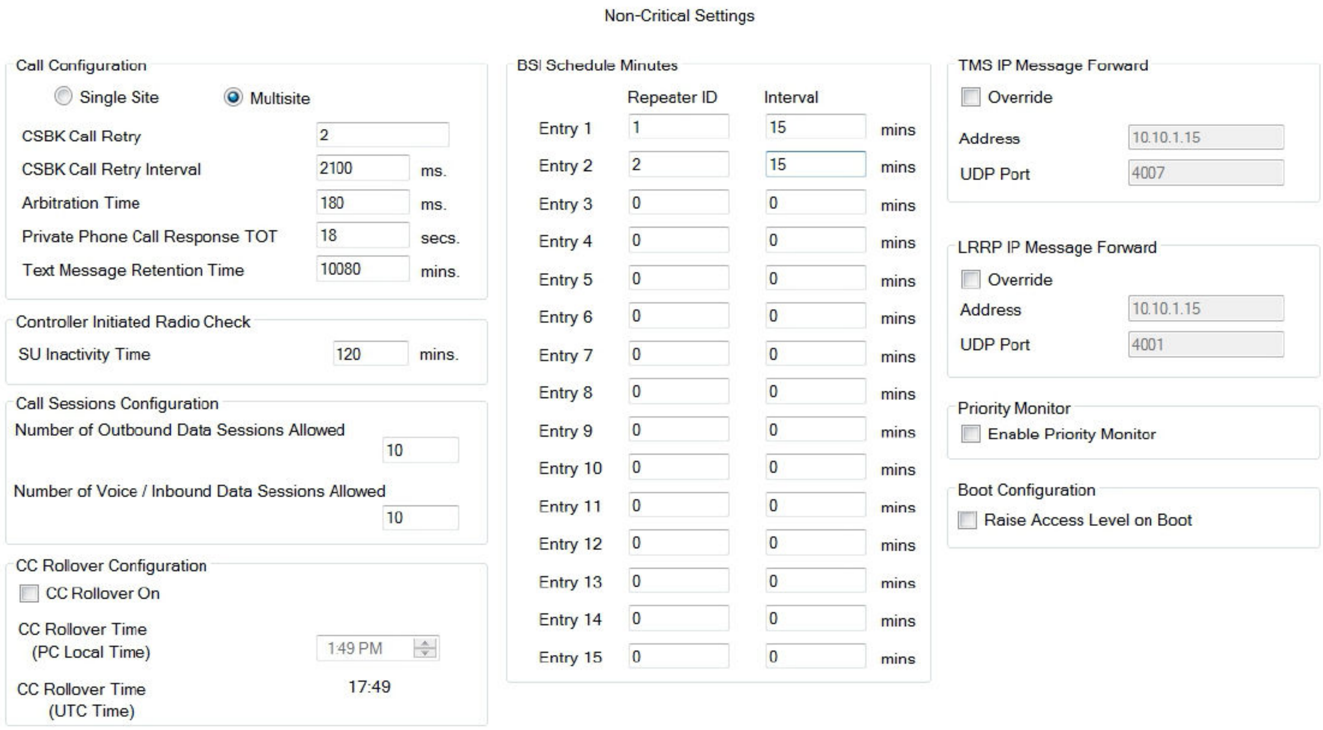
When a non-Control Channel repeater (operating in Fallback mode) is not repeating a call on either timeslot, it will periodically key-up to transmit the Fallback Beacon according to the Beacon Interval setting. During this transmission, the repeater sends the Fallback Beacon for the duration defined in Beacon Duration. If the Beacon Interval is set to 0 seconds (to indicate a continuous Beacon), the Beacon Duration is ignored and can be left at the default setting.

Maximum	18000 ms
Minimum	480 ms
Increment	120 ms
Default	480 ms

5.1.3.2 Site Settings – Non-Critical

The following figure shows an example of the **Non-Critical Settings** screen.

Figure 41: Non-Critical Settings Screen



Non-Critical Settings

Call Configuration

○ Single Site ● Multisite

CSBK Call Retry 2
CSBK Call Retry Interval 2100 ms.
Arbitration Time 180 ms.
Private Phone Call Response TOT 18 secs.
Text Message Retention Time 10080 mins.

Controller Initiated Radio Check

SU Inactivity Time 120 mins.

Call Sessions Configuration

Number of Outbound Data Sessions Allowed 10
Number of Voice / Inbound Data Sessions Allowed 10

CC Rollover Configuration

□ CC Rollover On
CC Rollover Time (PC Local Time) 1:49 PM
CC Rollover Time (UTC Time) 17:49

BSI Schedule Minutes

	Repeater ID	Interval	
Entry 1	1	15	mins
Entry 2	2	15	mins
Entry 3	0	0	mins
Entry 4	0	0	mins
Entry 5	0	0	mins
Entry 6	0	0	mins
Entry 7	0	0	mins
Entry 8	0	0	mins
Entry 9	0	0	mins
Entry 10	0	0	mins
Entry 11	0	0	mins
Entry 12	0	0	mins
Entry 13	0	0	mins
Entry 14	0	0	mins
Entry 15	0	0	mins

TMS IP Message Forward

□ Override
Address 10.10.1.15
UDP Port 4007

LRRP IP Message Forward

□ Override
Address 10.10.1.15
UDP Port 4001

Priority Monitor

□ Enable Priority Monitor

Boot Configuration

□ Raise Access Level on Boot

5.1.3.2.1 Call Configuration Parameters

5.1.3.2.1.1 Enabling Arbitration Time Field

The **Multisite** button should be enabled if this XRC is networked to another XRC, or to a XRT Gateway (a device that provides the interface to a wireline digital console, as well as certain airtime logging features).

Procedure:

Select the **Multisite** radio button.

5.1.3.2.1.2 CSBK Call Retry

This parameter determines the maximum number of retries attempted by the radio network if the destination radio does not respond to the first message for Private Call set-up, Remote Monitor set-up, Radio Check, Call Alert, Disable Command, or Enable Command.

NOTICE: This field should be configured with the same value in every XRT and XRC throughout the network. The requirement to use the same value network-wide is not enforced by the MOTOTRBO Connect Plus Network Manager software, but it must be followed for proper operation.

Minimum	0
Maximum	4
Increment	1
Default	2

5.1.3.2.1.3 CSBK Call Retry Interval (ms)

This parameter determines the interval that must expire before the device initiates a CSBK Call Retry.

NOTICE: This field should be configured with the same value in every XRT and XRC network-wide.

Minimum	600
Maximum	3600
Increment	1
Default	2100

5.1.3.2.1.4 Arbitration Time (ms)

In the event of near-simultaneous key-ups at different sites during the same call, arbitration increases the chances that the same audio is heard at all sites involved in the call.

NOTICE: This field should be configured with the same value in every XRT and XRC network-wide.

Minimum	120
Maximum	300
Increment	1
Default	180

5.1.3.2.1.5 Private Phone Call Response TOT (sec)

This parameter determines how long (in seconds) the XRC should attempt to contact (ring) a radio at the beginning of a Private Phone Call initiated by a phone user.

Minimum	8 secs
Maximum	60 secs
Increment	1 sec
Default	18 secs

5.1.3.2.1.6 Text Message Retention Time

This parameter determines how long the XRC Controller will retain an undelivered text message in the destination radio's text message mailbox. When the timer expires, the undelivered text message is deleted from the mailbox.

Minimum	1 minute
Maximum	10080 minutes (7 days)
Increment	1 minute
Default	10080 minutes (7 days)

5.1.3.2.2 Controller Initiated Radio Check Parameter

5.1.3.2.2.1 SU Inactivity Time (mins)

This parameter determines the SU inactivity time. The purpose of XRC-initiated radio check is to identify and deregister units that no longer require system resources.

The SU Inactivity Time parameter is set on a site-wide basis, but is tracked for each individual SU. The timer is reset whenever the XRC detects SU activity.

If the SU Inactivity Timer expires, and if the XRC shows that the SU is still registered to the site, the XRC sends at least one XRC Initiated Radio Check. Whether the XRC sends additional retries depends on how it is configured for CSBK Call Retries.

If the XRC finishes its Radio Check attempt (and any programmed retries), and receives no SU acknowledgment, the XRC deregisters the SU from the network.

Minimum	30 mins
Maximum	1440 mins
Increment	1 minute
Default	120 mins

5.1.3.2.3 Call Sessions Configuration

XRC has two programmable parameters used to determine how many calls in a particular category the controller will allow to be assigned at any one time. These parameters divide all non-emergency call types into two major categories as described in the following sub-sections.

NOTICE: Emergency Calls and Emergency Location Updates will always be assigned to an available time slot, regardless of how the two Call Sessions Configuration parameters have been configured.

5.1.3.2.3.1 Number of Outbound Data Sessions Allowed

This setting determines how many simultaneous sessions XRC will allow for call types in this category. The call types in this category are non-emergency location request/reports, text message delivery from XRC to a destination SU, Packet Data Call originated by an XRT Client and destined for a Connect Plus SU, and Connect Plus Over-the-Air (OTA) unconfirmed file transfer.

The XRC will continue to allocate time slots (if available) for calls in this category until the site reaches the configured value. If no time slots are available, or if the site reaches the configured value for **Number of Outbound Data Sessions Allowed**, subsequent calls in this category are not placed in the Busy Queue. For this reason, sites with a lot of outbound data activity (such as GPS updates) may wish to reserve one or more time slots specifically for outbound data. This will allow outbound data sessions to continue; even when all voice/inbound data slots are busy. For more information on how to set the Call Sessions Configuration parameters to achieve this objective, see the *MOTOTRBO Connect Plus System Planner*.

Minimum	0
Maximum	29
Increment	1
Default	29

5.1.3.2.3.2
Number of Voice/Inbound Data Sessions Allowed

This setting determines how many simultaneous sessions XRC will allow for call types in this category. The call types in this category are Group Call, Multigroup Call, Site All Call (voice), Private Call, and inbound data. At the current time, there is one call session classified as inbound data – text messages from the SU to the XRC.

The XRC will continue to allocate time slots (if available) for calls in this category until the site reaches the configured value. If no time slots are available, or if the site reaches the configured value for **Number of Voice/Inbound Data Sessions Allowed**, subsequent calls in this category are placed in the Busy Queue. This setting can be used in conjunction with the **Number of Outbound Data Sessions Allowed** parameter to effectively reserve a certain number of repeater time slots for calls in the "Outbound Data" and/or "Voice/Inbound Data" categories. For more information, see *MOTOTRBO Connect Plus System Planner*.

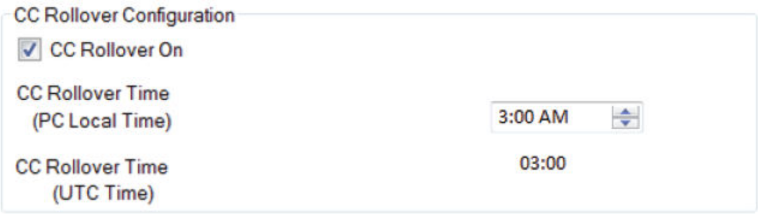
Minimum	0
Maximum	29
Increment	1
Default	29

5.1.3.2.4
Configuring Control Channel Rollover (Scheduled Rollover)

Scheduled Rollover is a daily event, and occurs as close to the scheduled time as possible. The actual Rollover Time depends partly on when repeater Timeslot 1 of the new Control Channel repeater becomes available (that is, not busy with a call). For additional important information about Control Channel Rollover, including information on how the Controller selects the next Control Channel repeater, see the *MOTOTRBO Connect Plus System Planner*.

When and where to use:
Up to four repeaters at a site may be designated as potential Control Channel Repeaters (see Control Channel List on page 87). When the Control Channel list has more than one repeater entry, Scheduled Control Channel Rollover can be enabled and configured.

Figure 42: CC Rollover Configuration Screen



CC Rollover Configuration

☑ CC Rollover On

CC Rollover Time (PC Local Time): 3:00 AM

CC Rollover Time (UTC Time): 03:00

The CC (Control Channel) Rollover Configuration settings are used to enable CC Rollover and to schedule a daily control channel rollover. When Site Configuration is opened, this screen shows the CC Rollover Time as presently set in the XRC. The CC Rollover Time entry field can be used to change the Rollover time, if desired.

Procedure:

1. Check the **CC Rollover On** checkbox to enable the CC Rollover feature and to enable the **CC Rollover Time** entry field. When the box is unchecked, there will be no CC Rollover (neither scheduled nor unscheduled CC Rollover).
2. Use the up/down arrow buttons next to the **CC Rollover Time** entry field to set the rollover time in PC Local Time. The configured PC Local Time converted to UTC (Universal Coordinated Time) appears in the area just below the setting window. Because the XRC keeps time in UTC, there is no automatic adjustment needed for changes due to Daylight Savings Time.
3. Save changes to the Site Configuration screen.

   The XRC will attempt to Rollover to one of the designated Control Channel repeaters at the scheduled time.

5.1.3.2.5 BSI Schedule Minutes Parameters

This parameter is used to configure which repeaters should send base station identification (and how often). The ID the repeater sends must be configured into the repeater with MOTOTRBO Board CPS.

IMPORTANT: Analog BSI (CWID) on the Control Channel Repeater disrupts the site operations and should be avoided if possible.

NOTICE: The ID that the repeater sends must be programmed into the repeater using MOTOTRBO CPS.

5.1.3.2.5.1 BSI Schedule Repeater ID

This parameter defines the Radio ID of the repeater that must send Base Station Identification (BSI). BSI is also called a Continuous Wave Identification (CWID).

Minimum	0
Maximum	15
Increment	1
Default	0

NOTICE: The list provides the ability to enter 15 Repeater IDs. Enter 0 for no updates.

5.1.3.2.5.2 BSI Interval

This parameter defines how often the repeater indicated by the Repeater ID field must send BSI (also called CWID).

Minimum	5 mins
Maximum	255
Increment	1 min

Default	0

NOTICE: The list provides the ability to enter 15 intervals. Enter 0 for no updates.

Repeaters operating in Auto Fallback Mode: When a repeater is operating in Auto Fallback mode, it utilizes the CWID TX Interval configured with MOTOTRBO CPS – not the BSI Interval configured with the Network Manager.

5.1.3.2.6 TMS IP Message Forward Parameters

5.1.3.2.6.1 Override

When this check box is unchecked (disabled), the XRC uses the TMS Server address extracted from IP messages sent by the TMS Server. This is the recommended configuration.

In multisite networks, where different sites have a different perspective back to the TMS Server, it is necessary to check (enable) the Override check box and configure the IP address that is correct from the perspective of this XRC.

For more information about when it is necessary to utilize the override feature, consult the *MOTOTRBO Connect Plus System Planner*.

5.1.3.2.6.2 Address

When "override" must be used, enter the TMS server IP address or URL that will be correct from the perspective of this device. The format for entering an IP address is (000-255).(000-255).(000-255).(000-255). If entering a URL, the device must be configured with a valid Nameserver under **Network** → **Settings**.

5.1.3.2.6.3 UDP Port

This parameter defines the server's LRRP UDP port that is correct from the perspective of this XRC.

NOTICE: This parameter is used only when the "override" must be used.

Minimum	4000
Maximum	65535
Increment	1
Default	0

5.1.3.2.7 LRRP IP Message Forward Parameters

5.1.3.2.7.1 Override

When this check box is unchecked (disabled), the XRC uses the LRRP Server address extracted from IP messages sent by the LRRP Server. This is the recommended configuration.

In multisite networks, where different sites have a different perspective back to the LRRP Server, it is necessary to check (enable) the Override check box and configure the IP address that is correct from the perspective of this XRC.

For more information about when it is necessary to utilize the override feature, consult the *MOTOTRBO Connect Plus System Planner*.

5.1.3.2.7.2 Address

When “override” must be used, enter the LRRP server IP address or URL that will be correct from the perspective of this controller. The format for entering an IP address is`<000-255>.<000-255>.<000-255>.<000-255>`. If entering a URL, the XRC must be configured with a valid Nameserver (reachable by this XRC) under **Network** → **Settings**.

5.1.3.2.7.3 UDP Port

This parameter defines the server's LRRP UDP port that is correct from the perspective of this XRC.

NOTICE: This parameter is used only when the "override" must be used.

Minimum	4000
Maximum	65535
Increment	1
Default	0

5.1.3.2.8 Priority Monitor checkbox

The **Priority Monitor** checkbox should be checked to enable the Priority Monitor Scan feature in this site controller. When the box is checked, Priority Monitor scan is enabled for any Group ID that has the **Enable Priority Monitor** checkbox enabled (checked) on its Group record.

When the box is unchecked, Priority Monitor scan is disabled at this site for all Group IDs, regardless of whether the **Enable Priority Monitor** checkbox is enabled (checked), or disabled (unchecked) on the Group record.

If the Network Manager user changes this setting to enable/disable Priority Monitor, the controller does not apply the new setting to calls in-progress when the setting is changed. It applies to subsequent calls only.

5.1.3.2.9 Raise Access Level On Boot checkbox

The **Raise Access Level On Boot** checkbox is checked if a large number of radios (100+) typically re-register with this site controller after device reboot.

When enabled, the site controller raises the site access level for at least one minute following reboot. This helps mitigate the number of registration collisions.

5.1.4

Configuring Fast GPS

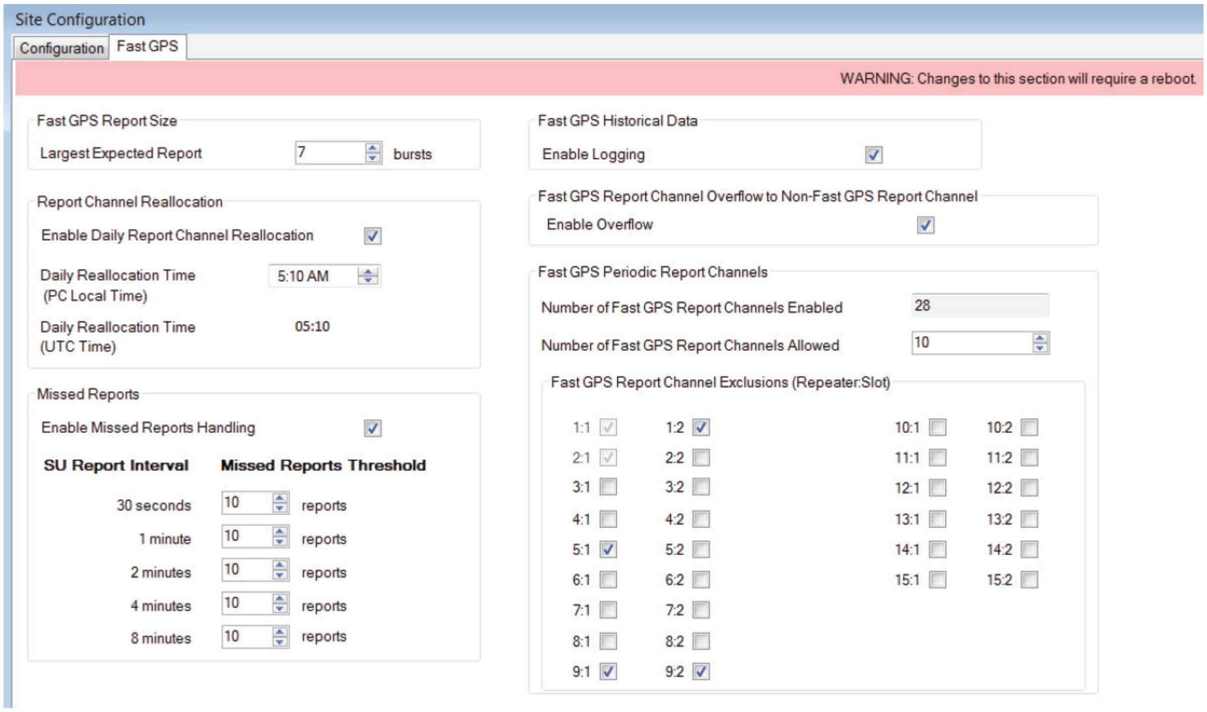
⚠ **CAUTION:** Changes to this section will require a reboot of the controller.

Procedure:

1. Click on **Settings** in Menu Bar.
2. Click on **Configuration** in menu.
3. Click on the **Fast GPS Tab**.

   The settings on the **Fast GPS Tab** can be edited when the connected XRC Controller has been enabled for one or more Fast GPS Report Channels. See Number of Fast GPS Report Channels Enabled on page 108 for more information.

Figure 43: Fast GPS Configuration Screen



Site Configuration

Configuration | Fast GPS

WARNING: Changes to this section will require a reboot.

Fast GPS Report Size
Largest Expected Report 7 bursts

Report Channel Reallocation
Enable Daily Report Channel Reallocation ☑
Daily Reallocation Time (PC Local Time) 5:10 AM
Daily Reallocation Time (UTC Time) 05:10

Missed Reports
Enable Missed Reports Handling ☑

SU Report Interval	Missed Reports Threshold
30 seconds	10 reports
1 minute	10 reports
2 minutes	10 reports
4 minutes	10 reports
8 minutes	10 reports

Fast GPS Historical Data
Enable Logging ☑

Fast GPS Report Channel Overflow to Non-Fast GPS Report Channel
Enable Overflow ☑

Fast GPS Periodic Report Channels
Number of Fast GPS Report Channels Enabled 28
Number of Fast GPS Report Channels Allowed 10

Fast GPS Report Channel Exclusions (Repeater:Slot)

1:1 ☑	1:2 ☑	10:1 □	10:2 □
2:1 ☑	2:2 □	11:1 □	11:2 □
3:1 □	3:2 □	12:1 □	12:2 □
4:1 □	4:2 □	13:1 □	13:2 □
5:1 ☑	5:2 □	14:1 □	14:2 □
6:1 □	6:2 □	15:1 □	15:2 □
7:1 □	7:2 □		
8:1 □	8:2 □		
9:1 ☑	9:2 ☑		

5.1.4.1

Fast GPS Report Size

5.1.4.1.1

Configuring Largest Expected Report

Procedure:

Configure the largest Fast GPS Report Size (in 60ms bursts) that will be transmitted by any radio enabled for Fast GPS that can use this site.

All Fast GPS Reports transmitted to the site must be equal to (or smaller than) this value. For instructions on how to determine a radio's Fast GPS Report Size, please see the *MOTOTRBO Connect Plus System Planner*.

Range	
Minimum	5 (bursts)
Maximum	10 (bursts)
Increment	1 (burst)
Default	10 (bursts)

5.1.4.2
Report Channel Reallocation

5.1.4.2.1
Daily Report Channel Reallocation Checkbox

This checkbox should be checked to enable Daily Report Channel Reallocation (if desired). After enabling the feature, use the **Daily Reallocation Time** field to schedule the time when Reallocation should begin each day. At the daily Reallocation time, the controller completes the current superframe in-progress, and then begins the Reallocation process. During the Daily Reallocation process, there will be no Fast GPS location reports for eight minutes. Instead, the Fast GPS radios re-register to obtain an updated Fast GPS Report Channel and Window assignment.

For more information on the operation and benefits of Daily Report Channel Reallocation, please see the *MOTOTRBO Connect Plus System Planner*.

5.1.4.2.2
Daily Reallocation Time

This is used to schedule the time when Reallocation should begin each day.

The controller begins Report Channel Reallocation as close to the scheduled time as possible (the controller must complete the current superframe before it starts transmitting the Reallocation superframe). While the controller is transmitting the special Reallocation superframe, the radios receive updated Fast GPS report channel and window assignments, but they do not send reports. It is recommended to schedule daily Reallocation during a time of day that has relatively low call activity, and when the gap in reporting will have the least impact.

For any site that has a scheduled time for Control Channel Rollover and a scheduled time for Fast GPS Report Channel Reallocation, it is recommended to schedule the Fast GPS Report Channel Reallocation at least 30 minutes prior to the Control Channel Rollover. This should provide sufficient time for the Fast GPS Report Channel Reallocation to complete prior to beginning the Control Channel Rollover.

5.1.4.2.2.1
Enabling Daily Reallocation Time

Procedure:

1 Check the **Enable Daily Report Channel Reallocation** checkbox to enable the feature and to enable the **Daily Reallocation Time** entry field.

2 Use the up/down arrow buttons next to the **Daily Reallocation Time** entry field to set the Daily Reallocation time in PC Local Time.

The configured PC Local Time, converted to UTC (Universal Coordinated Time) appears in the area just below the entry field. There is no automatic adjustment needed for changes due to Daylight Savings Time because the XRC keeps time in UTC.

3 Save changes when finished with configuration.

5.1.4.3 Missed Reports

5.1.4.3.1 Missed Reports Handling Checkbox

The controller-initiated Missed Reports Handling feature is enabled by checking this box. When this feature is enabled, the controller tracks how many consecutive Fast GPS reports it has missed from each radio assigned to a Fast GPS Report Channel.

If the number of missed reports hits the **Missed Reports Threshold** value that has been configured with the Network Manager for the radio’s Report Interval, the controller schedules a make-up report session on a normal traffic channel. The session will be assigned with a radio-specific Control Channel message. The traffic channel session will utilize an unconfirmed datagram to minimize the time required for the report. The controller will not schedule the traffic channel session if it knows the radio is involved in a call. Occasional missed reports are a normal part of Fast GPS operation and caution is recommended when enabling Missed Reports Handling and when configuring the **Missed Reports Threshold** value. If there are a large number of radios that must be scheduled for Missed Report sessions, this could have a detrimental impact on non-Fast GPS calls due to the competition for traffic channels and for Control Channel assignment messages. For more information, please see the *MOTOTRBO Connect Plus System Planner*.

5.1.4.3.2 Missed Reports Threshold Configuration

When Missed Reports Handling is enabled, the Missed Reports Threshold is configurable per Periodic Report Interval. When the radio has missed the configured number of consecutive Fast GPS Reports for its Report Interval, the controller schedules a make-up report session on a non-Fast GPS traffic channel as discussed above.

NOTICE: To determine the periodic report interval of radio, check the configuration of the location application software. It is not possible to determine the report interval of a radio by looking at the Network Manager, Connect Plus CPS, or the radio menu.

5.1.4.3.2.1 30 Seconds Setting

This setting determines the number of consecutive Fast GPS reports that must be missed by any radio with a 30-second report interval before the Controller schedules a make-up report session on a non-Fast GPS traffic channel.

Range	
Minimum	5 (reports)
Maximum	30 (reports)
Increment	1 (report)

Table continued…

Default	10 (reports)

5.1.4.3.2.2
1 minute Setting

This setting determines the number of consecutive Fast GPS reports that must be missed by any radio with a 1 minute report interval before the Controller schedules a make-up report session on a non-Fast GPS traffic channel.

Range	
Minimum	4 (reports)
Maximum	30 (reports)
Increment	1 (report)
Default	10 (reports)

5.1.4.3.2.3
2 minutes

This setting determines the number of consecutive Fast GPS reports that must be missed by any radio with a 2 minute report interval before the Controller schedules a make-up report session on a non-Fast GPS traffic channel.

Range	
Minimum	3 (reports)
Maximum	30 (reports)
Increment	1 (report)
Default	10 (reports)

5.1.4.3.2.4
4 minutes

This setting determines the number of consecutive Fast GPS reports that must be missed by any radio with a 4 minute report interval before the Controller schedules a make-up report session on a non-Fast GPS traffic channel.

Range	
Minimum	2 (reports)
Maximum	30 (reports)
Increment	1 (report)
Default	10 (reports)

5.1.4.3.2.5
8 minutes

This setting determines the number of consecutive Fast GPS reports that must be missed by any radio with a 8 minute report interval before the Controller schedules a make-up report session on a non-Fast GPS traffic channel.

Range	
Minimum	1 (report)
Maximum	30 (reports)
Increment	1 (report)
Default	10 (reports)

5.1.4.4
Fast GPS Historical Data

5.1.4.4.1
Logging Checkbox

When Fast GPS Historical logging is enabled (checked), the controller saves up to 100 MB of Fast GPS performance data for all Report Channels to the controller's hard disk. If the data exceeds 100 MB, the oldest data is automatically deleted and replaced with the newest data. To prevent data from the being lost, the Network Manager user can download the data from the hard disk to a computer before it is automatically deleted by the controller. When Fast GPS Historical logging is disabled (unchecked), the controller does not save Fast GPS performance data to the hard disk.

5.1.4.5
Fast GPS Overflow to Non-Fast GPS Channel

5.1.4.5.1
Overflow Checkbox

This setting determines the operation of the controller if it is not able to assign a Fast GPS-enabled radio to a Fast GPS Report Channel and Window (due to no available Window or Fast GPS Channel). If Overflow is enabled (box checked), the controller will make a best-effort to obtain location updates at the requested interval on a non-Fast GPS traffic channel. If Overflow is disabled (box unchecked), the controller will not attempt to obtain periodic location updates for the radio on a non-Fast GPS traffic channel. Upon scheduling the overflow session, the controller will create an Event Log entry to capture the SUID of the radio that could not be assigned to a Fast GPS Channel.

NOTICE: Caution is recommended if utilizing Fast GPS overflow. If there are a large number of SUs that cannot be assigned to a Fast GPS Report Channel, this could have a detrimental impact on non-Fast GPS calls due to the competition for traffic channels and for Control Channel assignment messages.

5.1.4.6
Fast GPS Periodic Report Channels

The settings in this section help determine how many repeater time slots (and which repeater time slots) the controller will select to use as Fast GPS Report Channels.

5.1.4.6.1 Number of Fast GPS Report Channels Enabled

This field displays the number of Fast GPS Report Channel timeslots that have been enabled (authorized) for this XRC Controller. The field cannot be edited by the Network Manager user. If the number of Fast GPS Report Channels enabled for this site needs to be increased, please contact your Motorola Solutions sales representative for more information.

The maximum number of Fast GPS Report Channels that will be allocated by the XRC at any given time is determined by the configurable setting called **Number of Fast GPS Report Channels Allowed**. The **Number of Fast GPS Report Channels Allowed** can be less than (or equal to) the **Number of Fast GPS Report Channels Enabled**, but it cannot be greater.

5.1.4.6.2 Number of Fast GPS Report Channels Allowed

This setting helps determine the maximum number of Fast GPS Report Channels that will be allocated by the XRC at any given time. The **Number of Fast GPS Report Channels Allowed** can be less than (or equal to) the **Number of Fast GPS Report Channels Enabled** for the site, but it cannot be greater. The number of Fast GPS Report Channels that the XRC allocates at any given time is also impacted by other factors, such as the configuration of the Fast GPS Report Channel Exclusions and by the number of eligible repeater channels that have checked-in with the controller. For any repeater on the site's Control Channel list, only repeater timeslot 2 is eligible to serve as a Fast GPS Report Channel.

Range	
Minimum	0
Maximum	See note
Increment	1
Default	0

NOTICE: The maximum number for Fast GPS Report Channels Allowed is the same number as displayed in the field called **Number of Fast GPS Report Channels Enabled**.

5.1.4.6.3 Fast GPS Report Channel Exclusions (Repeater:Slot)

Each checkbox represents a specific repeater time slot. The checkboxes are labeled 1:1 through 15:2. The number to the left of the colon is the Repeater Radio ID (1-15). The number to the right of the colon is the time slot number (1-2).

If any repeater time slot should **not** be allocated as a Fast GPS Report Channel, check its corresponding box. If a box is not checked, and if the repeater has checked in with the controller, the controller can allocate the corresponding time slot as a Fast GPS Report Channel if necessary.

For any repeater that is currently on the list of Control Channel repeaters (**Settings** → **Configuration**), the Network Manager automatically displays the corresponding box for time slot 1 of that repeater as checked and grayed out. It will not be used as a Fast GPS Report Channel.

NOTICE: Connect Plus repeaters must be numbered within the range of 1 to 15. The Network Manager displays all of these repeater numbers (1-15) on the Fast GPS Report Channel Exclusions list, regardless of whether a repeater with the corresponding number has checked in with the controller or not. It is not necessary to check boxes for repeater numbers that do not exist (and will not exist) on this site.

5.1.5 Configuring for Multisite (Multisite Networks Only)

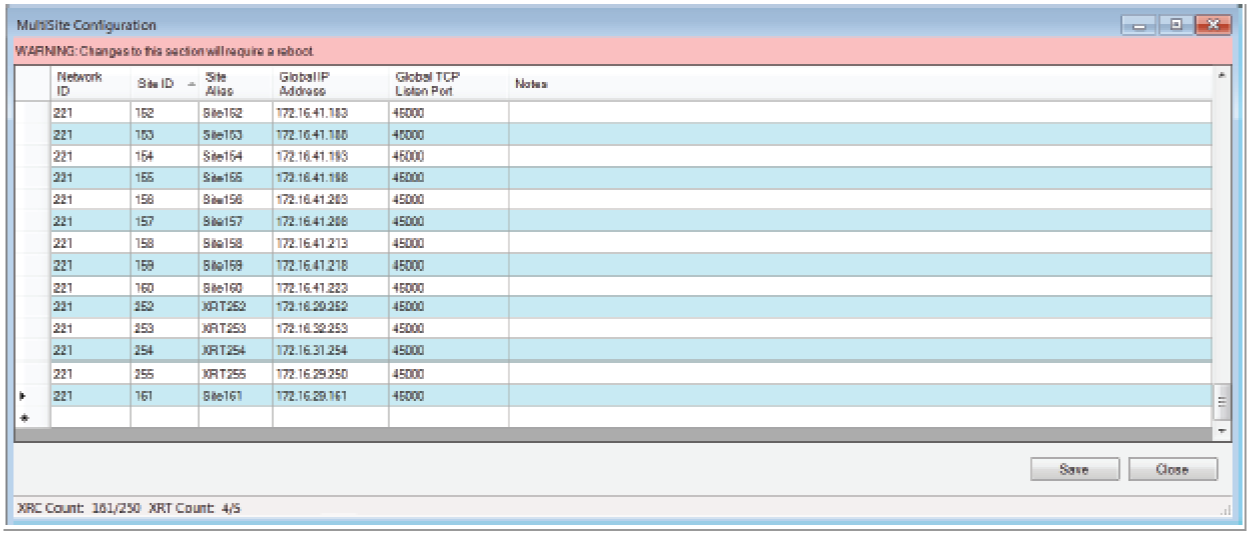
Procedure:

From the Menu Bar, select **Settings** → **Multisite**.

The **Multisite Configuration** window appears.

5.1.5.1 Multisite Settings

Figure 44: Multisite Configuration Window



MultiSite Configuration

WARNING: Changes to this section will require a reboot.

Network ID	Site ID	Site Alias	Global IP Address	Global TCP Listen Port	Notes
221	152	Site152	172.16.41.183	45000	
221	153	Site153	172.16.41.188	45000	
221	154	Site154	172.16.41.193	45000	
221	155	Site155	172.16.41.198	45000	
221	156	Site156	172.16.41.203	45000	
221	157	Site157	172.16.41.208	45000	
221	158	Site158	172.16.41.213	45000	
221	159	Site159	172.16.41.218	45000	
221	160	Site160	172.16.41.223	45000	
221	252	XRT252	172.16.29.252	45000	
221	253	XRT253	172.16.32.253	45000	
221	254	XRT254	172.16.31.254	45000	
221	255	XRT255	172.16.29.250	45000	
221	161	Site161	172.16.29.161	45000	

XRC Count: 161/250 XRT Count: 4/5

This screen tells the XRC Controller which other sites exist in the multisite network, and what IP address and TCP port to use for communicating with those sites. Do not enter IP information for the local site (that is, the site you are currently connected to) on this table. Local site IP information is configured under **Network** → **Settings**. The table should only include information for sites that are currently attached (or ready to attach) to the network. This table is also used to configure site numbers, IP addresses, and TCP ports for any XRT Gateway device that is part of the multisite network. The XRT Gateway is a device that provides the interface to a wireline console, as well as certain other features. If the XRC is enabled for the Multisite feature, it can be configured to communicate with up to two hundred forty-nine (249) other RF sites and up to five XRT Gateways.

NOTICE: Connect Plus currently supports a maximum of 250 RF sites in a multisite network. Each of these 250 sites is assigned a unique Site Number between 1 and 250. Whenever possible, assign site numbers in consecutive order. This is a recommendation for the sake of simplicity. It is not a requirement.

5.1.5.1.1 Saving Changes to the Multisite Configuration Screen

If the application user has edited any Multisite Configuration setting and attempts to Save, then the application displays the message `Are you sure you want to continue` to warn the user that the device must reboot to save the information. The message provides three buttons: **Yes**, **No**, and **Cancel**.

Procedure:

Perform one of the following actions:

- To save the changes and reboot the device, click **Yes**. This will disconnect the application from the device, and it will be necessary to re-connect after the reboot is complete (if desired).
- To close the Warning message and return to the **Multisite Configuration Screen**, click **No** or **Cancel**

5.1.5.1.2 Discarding Changes to the Multisite Configuration Screen

Procedure:

1. To close the Multisite Configuration Screen without saving changes, perform one of the following actions:
   - Click the **Close** button.
   - Click the **X** in the upper right-hand corner of the screen.

   If the application user has edited any information, then the application displays a message which advises that there are unsaved changes. The message asks, `Would you like to discard these changes and continue?`

2. Perform one of the following actions:
   - To discard the changes and close the **Multisite Configuration Screen**, Click **Yes**.
   - To close the message and return to the **Multisite Configuration Screen**, click **No** or **Cancel**.

5.1.5.1.3 List Items on the Multisite Configuration Screen

The lists are presented in table format (rows and columns). The left-most column is the **Row Header** column, which utilizes the following icons:

▶	**Right Facing Arrow Icon** Indicates that the row, or a cell within the row, has been selected for editing.
✎	**Pencil Icon** Indicates that a cell within the row is being edited.
✳	**Asterisk Icon** Indicates a new row in the list. (See information below on “Creating a new row in the list.”).

Creating a new row in the list

The application automatically adds a new row to the end of the list when the application user enters data into the previous row. If the application cannot create a new row (because the list has the maximum number of entries), the asterisk icon disappears when the user enters data in the last row of the list.

NOTICE: The bottom left-hand corner of the **Multisite Corner** of the **Multisite Screen** displays two counts:

XRC Count: x/y
XRT Count: x/y
x = The number of devices currently on the list.
y = The number of devices that can be placed on the list.

Entering information in cell

To enter or edit information in a cell, navigate to the desired cell, and then edit as desired.

Delete a row from the list

To delete a row from the list, highlight the entire row by clicking on the left-most column in the row, and then press the DELETE key on the computer keyboard.

5.1.5.1.4

Network ID Parameters

This parameter defines the Network ID transmitted over-the-air by the network site referenced by this entry. The network ID must be the same network-wide, and must match the Network ID programmed into Connect Plus devices using this network.

Minimum	1
Maximum	4095
Increment	1
Default	Network ID (sets in **Settings** → **Configuration** → **Site Network ID**)

5.1.5.1.5

Site ID

This parameter defines the site number of the device referenced by this entry.

NOTICE: Site numbers 1 through 250 can be assigned to RF sites only. (An RF site has an XRC Controller and one or more repeaters). Site numbers 251 through 255 can be assigned to XRT Gateways. If the XRC is not enabled for the Multisite feature, it cannot network to other RF sites, but it can network to a single XRT, which must be configured as Site 255 on this screen.

Minimum	1 for an RF site, 251 for an XRT Gateway
Maximum	250 for an RF site, 255 for an XRT Gateway
Increment	1
Default	Blank

5.1.5.1.6

Site Alias

This field is to be entered with the alias of the XRC Controller or XRT Gateway referenced by this entry. The field supports up to 255 bytes of data.

5.1.5.1.7

Global IP Address

Connect Plus utilizes TCP/IP to send call set-up messages and other control messages between network sites. Connect Plus utilizes UDP/IP for audio routing.

The IP address entered into this field is used for UDP/IP communications with the site represented by the entry. If the site represented by this entry has a lower site number than the site that is being configured, then the entered IP address is also used when this site contacts the lower-numbered site to initiate the TCP/IP socket. If the site represented by this entry has a higher site number than the site is being configured, then the higher numbered site will initiate the TCP/IP socket, based on the information configured into its Multisite Table.

The Global IP address could be either a private or public IP address, depending on whether the device configured site is located in the same LAN as the site referenced by this entry. The format and range for the address are ***<(000-255)>.<(000-255)>.<(000-255)>.<(000-255)>***.

5.1.5.1.8 Global TCP Port

This parameter defines the port number used to reach the TCP Control Port of the network site referenced by this entry.

Minimum	1
Maximum	65535
Increment	1
Default	Blank

5.1.5.1.9 Notes

This field allows the user to create a note (alphanumeric string) about the network site corresponding to this entry. The maximum number of characters is 255.

NOTICE: This field is optional.

Chapter 6

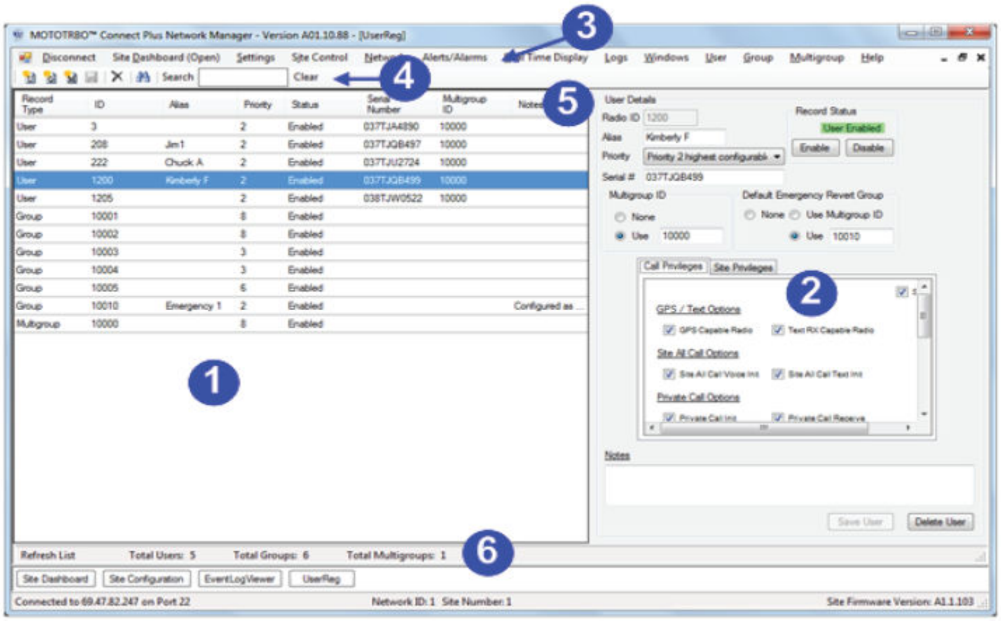
System Management

6.1 Provisioning and Configuring Connect Plus Subscribers

This section describes how user records are created, configured, and (if necessary) removed. See the *MOTOTRBO Connect Plus System Planner* for a complete description of Connect Plus Fleetmap Development.

The **User Registration** window appears when the **Users** option is selected from the **Settings** menu.

Figure 45: User Registration Window



Record Type	ID	Alias	Priority	Status	Serial Number	Multigroup ID	Notes
User	3		2	Enabled	037TJA4890	10000	
User	208	Jim1	2	Enabled	037TJQB497	10000	
User	222	Chuck A	2	Enabled	037TJU2724	10000	
User	1200	Kimberly F	2	Enabled	037TJQB499	10000	
User	1205		2	Enabled	038TJW0522	10000	
Group	10001		8	Enabled			
Group	10002		8	Enabled			
Group	10003		3	Enabled			
Group	10004		3	Enabled			
Group	10005		6	Enabled			
Group	10010	Emergency 1	2	Enabled			Configured as ...
Multigroup	10000		8	Enabled			

User Details
Radio ID 1200
Alias Kimberly F
Priority Priority 2 highest configurable
Serial # 037TJQB499

Record Status
User Enabled

Multigroup ID
○ None
● Use 10000

Default Emergency Revert Group
○ None ○ Use Multigroup ID
● Use 10010

GPS / Text Options
☑ GPS Capable Radio ☑ Text RX Capable Radio

Site All Call Options
☑ Site All Call Voice Init ☑ Site All Call Text Init

Private Call Options
☑ Private Call Init ☑ Private Call Receive

Notes

Total Users: 5 Total Groups: 6 Total Multigroups: 1

Connected to 69.47.82.247 on Port 22 Network ID: 1 Site Number: 1 Site Firmware Version: A1.1.103

1 Display Area – shows a list of one or more user records.

2 Details Area – shows the details of the user record that is selected in the Display Area.

3 Menu Bar

4 Submenu Bar

5 Header

6 Display Area Totals

The Details Area

Whenever a user record (Unit, Group, or Multigroup) is saved with the Network Manager, the XRC of the site where the change was made sends a time-stamped copy of that user record to all Connect Plus sites in its Multisite list. Even if one of those sites is currently offline, it will receive a copy of the updated record once the network communication is re-established. Through this automatic mechanism, the network strives to keep the user database of all Connect Plus sites in synch.

In regards to managing the Connect Plus user database, the Network Administrator should be aware of the following important points:

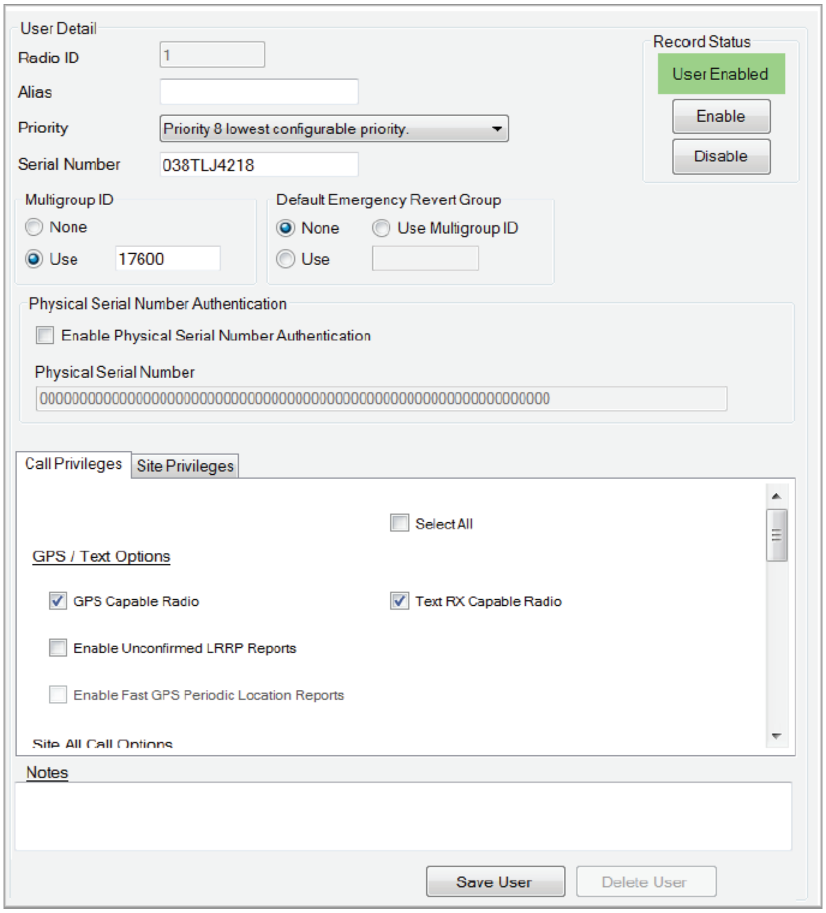
- While the Connect Plus design allows user records to be edited through any Connect Plus site, simultaneously editing the user database at two different sites should be discouraged. If the same record is simultaneously (or near-simultaneously) edited and saved at two different sites, it is possible for those sites to have different information about the same record.
- It is strongly recommended that the Network Administrator designate one Connect Plus site as the preferred site for making changes to the user database. This information should be communicated to all persons who will be adding and/or editing user records. Establishing this policy decreases the chances that two different people will simultaneously (or near simultaneously) edit and save the same user record at two different network sites.
- Do not leave the Network Manager’s **User Registration** window open for long periods of time when not actively working with the user database. The window is not automatically refreshed with user database changes that are made:
  - by another PC that may be connected to this same network site
  - by another PC connected to a different network site
  - changes that are made to user records based on "disable" or "enable" commands that are sent by authorized radio users over-the-air.

  If the **User Registration** window is left open for an extended period of time, always click **Refresh List** in the lower left-hand corner of the User Registration window before viewing or editing user records. This causes the Network Manager to download the user records again and update the display with the current information.
- The number of records supported by the Connect Plus user database depends on the record type, and whether it is the database for a single site or multisite system.
  - The record for an individual radio is called a "user record" by the MOTOTRBO Connect Plus Network Manager. This record type is also commonly known as a "unit record", "UID" or "Radio ID". Connect Plus supports 48,000 such records for a single site system and 60,000 records for a multisite system.
  - The combined total of Group and Multigroup records supported by Connect Plus is 4,000 for a single site system and 16,000 for a multisite system.

6.1.1 User Details

The following figure shows the interface used for entering user details.

Figure 46: User Details Screen



User Detail

Radio ID: 1

Alias:

Priority: Priority 8 lowest configurable priority.

Serial Number: 038TLJ4218

Multigroup ID: ○ None ● Use 17600

Default Emergency Revert Group: ● None ○ Use Multigroup ID ○ Use

Record Status: User Enabled

Physical Serial Number Authentication

□ Enable Physical Serial Number Authentication

Physical Serial Number: 0000000000000000000000000000000000000000000000000000000000000000

□ Select All

GPS / Text Options

☑ GPS Capable Radio ☑ Text RX Capable Radio

□ Enable Unconfirmed LRRP Reports

□ Enable Fast GPS Periodic Location Reports

Site All Call Options

Notes

6.1.1.1

Radio ID

This parameter defines the Radio ID (SUID) of the MOTOTRBO Subscriber Unit corresponding to this record.

Minimum	1
Maximum	16,776,351
Increment	1
Default	1

6.1.1.2

Alias

This parameter defines the alphanumeric alias of the MOTOTRBO Subscriber Unit corresponding to this record.

Minimum	-
Maximum	255 characters
Increment	-

Table continued…

Default	Blank

6.1.1.3 Configuring User Status

This section displays and enables to change the status of the user record for this Radio ID.

Procedure:

Perform one of the following actions:

- To enable the XRC to send the Enable Command (when the unit is registered into the network), click the **Enable** button.
- To enable the XRC to send the Disable Command (when the unit is registered into the network), click the **Disable** button.

- If the **Enable** button is clicked, the record displays as `User Enabled (green)`.
- If the **Disable** button is clicked, the record displays as `User Disabled (red)`.

6.1.1.4 Priority

This parameter defines the priority level of the radio, Group or Multigroup ID corresponding to this record. It is used for prioritizing calls in Busy Queue.

The range of the priority level is from 2 to 8: **Priority 2** is the highest, and **Priority 8** is the lowest configurable priority.

6.1.1.5 Serial Number

This parameter defines the 10-character MOTOTRBO Serial Number for the radio corresponding to this record.

If a serial number is entered, that does not conform to the expected serial number format, an exclamation point (`!`) in a red circle appears next to the field. Pass the cursor over the circle to display the error and an example of a valid serial number.

6.1.1.6 Multigroup ID

This parameter defines the Multigroup ID programmed into the Connect Plus Option Board for this radio unit. The XRC automatically provides audio for this ID at any network site where this radio registers. To enter the Multigroup ID for this radio, select the bullet labeled **Use**, and then enter the Multigroup ID in the field to the right. There must already be a Multigroup record that matches this ID in the user database. If this radio does not use a Multigroup ID, select the bullet labeled **None**.

Minimum	1
Maximum	16,776,351
Increment	1
Default	Blank

NOTICE: If a Multigroup ID number is entered that does not conform to the expected Multigroup number format, an exclamation (!) mark in a red circle is displayed next to the field. Pass the cursor over the circle to display the error and an example of a valid Multigroup ID number.

6.1.1.7 Configuring Default Emergency Revert Group

Prerequisites: In order to correctly configure Default Emergency Revert Group, it is necessary to know how the subscriber unit has been (or will be) programmed with Connect Plus CPS. If this radio is authorized to initiate an Emergency Call or Emergency Alert, it is necessary to enable the **Emergency Init** checkbox.

Procedure:

1 Depending on how the radio has been programmed, select one of the following:

- **None**

If the radio is not configured to initiate or initiate an Emergency Call or Emergency Alert in any Connect Plus zone, or if the radio is configured with Connect Plus CPS to always initiate Emergency Calls using its Selected Talk Group.

- **Use Multigroup ID**

If the radio is configured to initiate Emergency Calls on its Default Emergency Revert Group ID, and the Default Emergency Revert Group ID is set to **Multigroup** in Connect Plus CPS programming.

Use

If the radio is configured with Connect Plus CPS to initiate or receive an Emergency Alert or Emergency Call on its Default Emergency Revert Group ID, and the Default Emergency Revert Group ID is configured for something other than its Multigroup ID.

2 After selecting the bullet labeled **Use**, enter the Group ID into the field to the right of the bullet. This must match the Default Emergency Revert Group ID programmed into the radio with Connect Plus CPS, and there must be a Group record for this ID in the controller database.

6.1.1.8 Registration Authentication

Beginning with Connect Plus System Release 1.6, the type of serial number that the radio sends when authenticating with the Connect Plus system is configurable per subscriber unit. The choices are **MOTOTRBO Serial Number Authentication** or **Physical Serial Number Authentication**.

- **MOTOTRBO Serial Number Authentication** was used exclusively prior to System Release 1.6, and remains the default method. See MOTOTRBO Serial Number Authentication on page 117.
- **Physical Serial Number Authentication** is a highly secure method that is available beginning with Connect Plus System Release 1.6. See Enabling Physical Serial Number Authentication on page 118 and Entering the Physical Serial Number on page 118.

IMPORTANT: The authentication method configured in the Connect Plus Option Board Codeplug (using MOTOTRBO Connect Plus CPS) and the authentication method configured in the Connect Plus user record for the same radio (using the MOTOTRBO Connect Plus Network Manager) must agree.

6.1.1.8.1 MOTOTRBO Serial Number Authentication

When the **Enable Physical Serial Number Authentication** box is unchecked (which is the default setting), MOTOTRBO Serial Number Authentication is enabled and expected. In this case, enter the Serial Number of the radio as described in Serial Number on page 116

6.1.1.8.2
Enabling Physical Serial Number Authentication

This checkbox tells the site controllers which type of authentication to expect from the radio corresponding to this record. It is also used to activate the **Physical Serial Number** entry field.

Procedure:

Check the **Enable Physical Serial Number Authentication** box to enable Physical Serial Number Authentication and to activate the **Physical Serial Number Entry** field.

Unchecking this box grays out the **Physical Serial Number Entry** field. If a Physical Serial Number is entered into the field prior to unchecking the box, it will be preserved. When the **Enable Physical Serial Number Authentication** box is unchecked in the User Record, the radio can still authenticate with its Physical Serial Number if the radio's correct Physical Serial Number has been entered into the Physical Serial Number entry field on the user record. This is allowed to help facilitate migration from MOTOTRBO Serial Number Authentication to Physical Serial Number Authentication, but is not recommended for long-term operation. For more information on migrating an existing radio from MOTOTRBO Serial Number Authentication to Physical Serial Number Authentication, see the *MOTOTRBO Connect Plus System Planner*.

When the **Enable Physical Serial Number Authentication** box is checked, if the radio attempts to authenticate using its MOTOTRBO Serial Number, the registration is **not** allowed. The controller will deny the registration and generate an Event Log entry.

6.1.1.8.3
Entering the Physical Serial Number

The Physical Serial Number is unique for every Connect Plus subscriber radio. It is expressed with 64 hexadecimal characters, and it must be entered into the user record exactly as it appears after reading the radio with MOTOTRBO CPS. For this reason, the “copy and paste” method is strongly recommended for transferring the number from MOTOTRBO CPS to the MOTOTRBO Connect Plus Network Manager.

Prerequisites: After obtaining the Physical Serial Number of the radio, enter the Physical Serial Number into the user record of the radio in the Connect Plus user database as follows:

Procedure:

1. Enable the Physical Serial Number entry field on the user record corresponding to the radio by checking the **Enable Physical Serial Number Authentication** checkbox.

   By default, the Network Manager populates the Physical Entry Number entry field with a string of 64 zeroes.

2. Perform one of the following actions to replace the default string with the Physical Serial Number of the radio:
   - Copy and paste method (recommended):
     1. Copy the desired Physical Serial Number from MOTOTRBO CPS (or from a document containing the number).
     2. Use the cursor to select and highlight the character string in the **Physical Serial Number** field.
     3. Paste the Physical Serial Number from the memory of the computer into the **Physical Serial Number** entry field.
   - Use the computer keyboard to enter the Physical Serial Number. (This method is not recommended due to the risk of input errors (when compared to the copy and paste method):

1. Use the cursor to select and highlight the character string in the Physical Serial Number field.
2. Press the delete key to remove the current string.
3. Enter the Physical Serial Number using the keyboard. The Physical Serial Number must be 64 characters long. The following hexadecimal characters are allowed: 0-9, A-F.

Regardless of which input method is utilized, when the cursor is moved away from the Physical Serial Number entry field, the Network Manager checks to see if the Physical Serial Number conforms to the expected format. If it does not conform to the expected format, the Network Manager displays an error message.

6.1.1.8.4 Saving a User Record Containing a Physical Serial Number

When the Network Manager user attempts to save a user record containing a Physical Serial Number (after completing all edits to the record), the system checks the Physical Serial Number against all other Physical Serial Numbers already in the database of the controller. If there is a conflict in any key portion of the Physical Serial Number, the Network Manager displays a message that the record cannot be saved due to Physical Serial Number Conflict. The message contains the SUID of the user record with the conflicting Physical Serial Number. The Network Manager will not allow the record to be saved until the conflict is resolved.

The Physical Serial Number conflict may not be apparent by simply inspecting the Physical Serial Number in the conflicting record. Physical Serial Numbers can be in conflict even though the numbers may not be completely identical. The best way to resolve the conflict is re-enter both Physical Serial Numbers in the Connect Plus user database, exactly as they appear in MOTOTRBO CPS after reading the radios. This will resolve the conflict.

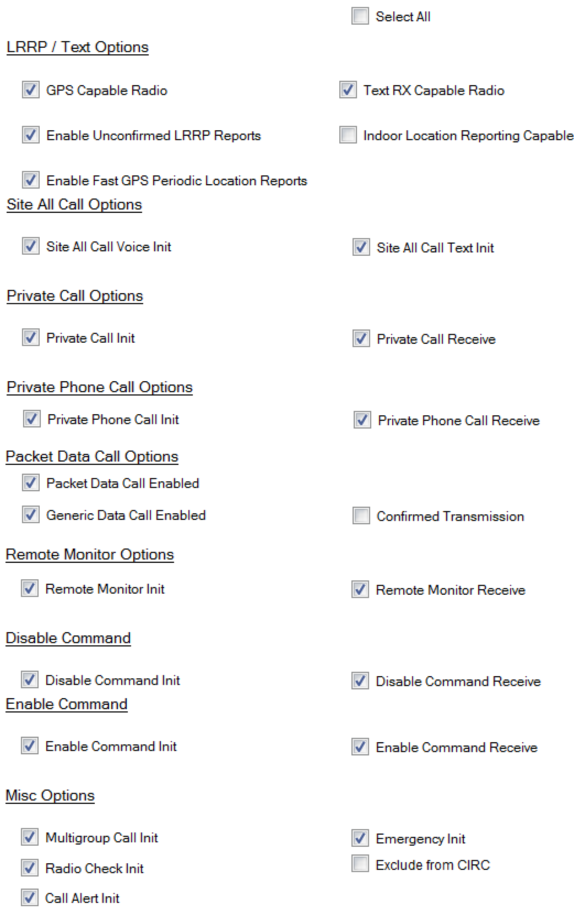
If you do not have enough information to immediately resolve the conflict (by entering a non-conflicting Physical Serial Number) then you can delete the entered Physical Serial Number, returning the field to its default value (all zeroes). After the field returns to its default value, uncheck the box **Enable Physical Serial Number Authentication**. You must obtain a valid, non-conflicting, Physical Serial Number prior to enabling Physical Serial Authentication for this user.

6.1.2 User Details Check Boxes

Some of the User Details check boxes apply to radio users only. They are:

- **GPS Capable Radio**
- **Enable Unconfirmed LRRP Reports**
- **Enable Fast GPS Periodic Location Updates**
- **Indoor Location Reporting Capable**
- **Text RX Capable Radio**
- **Site All Call Text Init**
- **Private Phone Call Init**
- **Private Phone Call Receive**
- **Exclude from CIRC**

Figure 47: User Details Check Boxes Screen



□ Select All

LRRP / Text Options

☑ GPS Capable Radio ☑ Text RX Capable Radio

☑ Enable Unconfirmed LRRP Reports □ Indoor Location Reporting Capable

☑ Enable Fast GPS Periodic Location Reports

Site All Call Options

☑ Site All Call Voice Init ☑ Site All Call Text Init

Private Call Options

☑ Private Call Init ☑ Private Call Receive

Private Phone Call Options

☑ Private Phone Call Init ☑ Private Phone Call Receive

Packet Data Call Options

☑ Packet Data Call Enabled

☑ Generic Data Call Enabled □ Confirmed Transmission

Remote Monitor Options

☑ Remote Monitor Init ☑ Remote Monitor Receive

Disable Command

☑ Disable Command Init ☑ Disable Command Receive

Enable Command

☑ Enable Command Init ☑ Enable Command Receive

Misc Options

☑ Multigroup Call Init ☑ Emergency Init

☑ Radio Check Init □ Exclude from CIRC

☑ Call Alert Init

6.1.2.1 Selecting All

Procedure:

To automatically select all of the options underneath, check this box .

6.1.2.2 GPS Capable Radio

When the radio corresponding to this record is equipped with an internal GPS unit and the GPS checkbox is enabled in the codeplug of the radio with MOTOTRBO CPS, check this box.

Beginning with Connect Plus System Release 1.5, if a radio informs the controller via over-the-air messaging that the radio is not GPS capable, the controller will automatically uncheck (disable) the **GPS Capable Radio** checkbox on the user record of the radio. This occurs if the controller attempts to obtain a location report, but the radio is not is equipped with GPS hardware, or (in some models) if the GPS checkbox has been disabled in the radio's codeplug with MOTOTRBO CPS. The controller will also automatically uncheck (disable) the **GPS Capable Radio** checkbox if the **Enable Unconfirmed LRRP Reports** flag is enabled on the user record, but controller determines that Unconfirmed LRRP is not supported by the current Option Board firmware of the radio. To obtain LRRP reports from the radio, it will be necessary to disable (uncheck) the **Enable Unconfirmed LRRP Reports** flag or to upgrade the Connect Plus Option Board firmware.

6.1.2.3

Unconfirmed LRRP Reports

Unconfirmed LRRP (Location Request Response Protocol) reports for the radio corresponding to this record is enabled when this box is checked.

When enabled, the radio transmits all location reports via unconfirmed datagrams (one attempt per session). Unconfirmed transmission provides greater overall system throughput (more reports per channel). To utilize Unconfirmed LRRP Reports, the Connect Plus Option Board firmware must be at Connect Plus System Release 1.6 (or later). The box must not be checked if the Option Board firmware is prior to Connect Plus Release 1.6. When disabled (unchecked), the radio transmits Location reports via confirmed datagrams (up to three attempts per report session, if necessary). This was the method for transmitting all Connect Plus location reports prior to System Release 1.6, and it continues to be supported.

NOTICE: This box must be checked for any radio that is enabled for Fast GPS Periodic Location reports on its user record. However, a radio with Option Board with firmware from Release 1.6 (or later) can utilize unconfirmed LRRP, even if it is not enabled for Fast GPS.

6.1.2.4

Enabling Fast GPS Periodic Location Reports

Prerequisites: In order to use Fast GPS Location Reports, please ensure that:

- the Connect Plus Option Board firmware must be at Connect Plus System Release 1.6 (or later) to utilize Fast GPS
- that Unconfirmed LRRP must be enabled (checked) prior to enabling Fast GPS Periodic Location Reports
- the site must be enabled (authorized) for one or more Fast GPS Report Channels.

Procedure:

Check this box for any radio that should transmit Periodic Location Reports via the Connect Plus Fast GPS Report Channel method.

6.1.2.5

Indoor Location Reporting Capable

Check this checkbox when the radio corresponding to this record supports and utilizes the Indoor Location feature

If a radio is configured for Indoor Location, but the controller detects that its firmware does not support the feature, the XRC automatically unchecks (disables) the **Indoor Location Reporting Capable** checkbox on the user record of the radio.

6.1.2.6

Text RX Capable Radio

If the radio corresponding to this record is capable of displaying received text messages, this box should be checked. When this box is unchecked, the controller will not accept a text message that is targeted to this radio's individual ID. If a text message is targeted to a Group ID of interest, this radio will receive the text message (like other group members), but a non-display portable or numeric display mobile will not display the message, store the message, or notify the user that one has been received.

6.1.2.7
Authorizing Site All Call Voice

Procedure:

If the radio corresponding to this record is authorized to initiate a voice transmission to the Site All Call Voice ID, check this box.

6.1.2.8
Authorizing All Call Text Init

Procedure:

Check this box if the radio corresponding to this record is authorized to send a text message to the Site All Call Text ID.

6.1.2.9
Authorizing Private Call Init

Procedure:

Check this box if the radio corresponding to this record is authorized to initiate Private Calls.

6.1.2.10
Authorizing Private Call Receive

Procedure:

Check this box if the radio corresponding to this record is authorized to receive Private Calls.

6.1.2.11
Authorizing Private Phone Call Init

Procedure:

Check this box if the radio corresponding to this record is authorized to initiate Private Phone Calls.

6.1.2.12
Authorizing Private Phone Call Receive

Procedure:

Check this box if the radio corresponding to this record is authorized to receive Private Phone Calls.

6.1.2.13
Authorizing Packet Data Calls

Procedure:

Check this box if the radio corresponding to this record is authorized to initiate and receive Packet Data Calls.

6.1.2.14 Authorizing Generic Data Call

Procedure:

Check this box if the radio corresponding to this record is authorized to initiate and receive Generic Data Calls.

6.1.2.15 Enabling Confirmed Transmission

When Generic Data Call is enabled, this box determines whether the controller utilizes the confirmed or unconfirmed transmission method when sending Generic Data Call packets to this subscriber radio.

Procedure:

Perform one of the following actions:

- Check this box to instruct the controller to utilize confirmed data transmission.
- Uncheck this box to instruct the controller to utilize unconfirmed data transmission.

6.1.2.16 Authorizing Remote Monitor Init

Procedure:

Check this box if the radio corresponding to this record is authorized to monitor a remote radio.

The remote radio is not aware that it is being monitored.

6.1.2.17 Authorizing Remote Monitor Receive

Procedure:

Check this box when the radio corresponding to this record is allowed to be monitored by another SU. The radio will not be aware that it is being monitored.

6.1.2.18 Authorizing Disable Command Init

Procedure:

Check this box if the radio corresponding to this record is authorized to send a command to disable a remote radio.

6.1.2.19 Authorizing Disable Command Receive

Procedure:

Check this box if the radio corresponding to this record is allowed to be disabled by a remote radio.

The XRC is authorized to disable any radio, regardless of whether this box is checked or not.

6.1.2.20 Authorizing Enable Command Init

Procedure:

Check this box if the radio corresponding to this record is authorized to send an Enable Command to a remote radio (one that was previously disabled).

6.1.2.21 Authorizing Enable Command Receive

Procedure:

Check this box if the radio corresponding to this record is allowed to be enabled by a remote radio.

The XRC is authorized to enable any radio, whether this box is checked or not.

6.1.2.22 Authorizing Multigroup Call Init

Procedure:

Check this box if the radio corresponding to this record is authorized to initiate a Multigroup Call. This permission applies to both voice calls and text messages to the Multigroup ID.

6.1.2.23 Authorizing Radio Check Init

Procedure:

When the subscriber corresponding to this record is authorized to Radio Check a remote radio, check this box.

6.1.2.24 Authorizing a Call Alert Init

Procedure:

Check this box if the radio corresponding to this record is authorized to initiate a Call Alert to a remote radio.

6.1.2.25 Authorizing Emergency Init

Procedure:

Check this box when the radio corresponding to this record is authorized to initiate an Emergency Call or Emergency Alert.

6.1.2.26 Exclude From CIRC

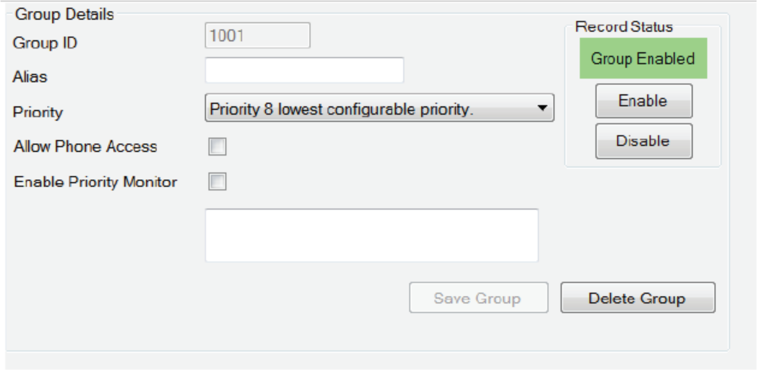
When the box is checked, the Controller will not perform a Controller Initiated Radio Check (CIRC) on the radio corresponding to this record, regardless of how long the radio has been inactive on the system. Because the controller does not perform the radio check, it will not deregister the unit due to a failed radio check.

6.1.2.27
Notes

This field allows the user to create a note (alphanumeric string) about the radio, Group or Multigroup. The maximum number of characters is 255.

6.1.3
Group Details Screen

Figure 48: Group Details Screen



Group Details
Group ID: 1001
Alias:
Priority: Priority 8 lowest configurable priority.
Allow Phone Access ☐
Enable Priority Monitor ☐

Record Status: Group Enabled

6.1.3.1
Group ID

This parameter defines the Group ID for this record.

Minimum	1
Maximum	16,776,351
Increment	1
Default	Blank

NOTICE: If a Group number is entered that does not conform to the expected Group number format, an exclamation (`!`) mark in a red circle is displayed next to the field. Pass the cursor over the circle to display the error and an example of a valid Group number.

6.1.3.2
Alias

This parameter defines the alphanumeric alias of the MOTOTRBO Subscriber Unit, Group or Multigroup. The maximum number of characters is 255.

6.1.3.3
Record Status

This section displays and enables to change the status of the user record for this Group or Multigroup ID.

Perform one of the following actions:

- Click **Enable** to display the record as Group Enabled (green).
- Click **Disable** to display the record as Group Disabled (red).

NOTICE: There is no over-the-air command sent when the buttons are clicked. The change is enforced the next time a radio user attempts to initiate a call or text using the Group ID or Multigroup ID.

6.1.3.4 Priority

This parameter defines the priority level of the radio, Group or Multigroup ID corresponding to this record. It is used for prioritizing calls in Busy Queue.

The range of the priority level is from 2 to 8: **Priority 2** is the highest, and **Priority 8** is the lowest configurable priority.

6.1.3.5 Allowing Phone Access

Procedure:

Check (enable) this box if a Telephone User should be allowed to access this Group or Multigroup.

6.1.3.6 Priority Monitor

Checking this box enables Priority Monitor announcements for this Group ID.

The Group record should be enabled for Priority Monitor if the corresponding Group ID is configured as a Priority One or Priority Group in any Connect Plus radio, network-wide. Also, if any radio is configured to initiate and receive Emergency voice calls on its Default Emergency Group ID, and if the System Administrator desires the controller to make priority announcements for this Group, then check this box on the corresponding Group record.

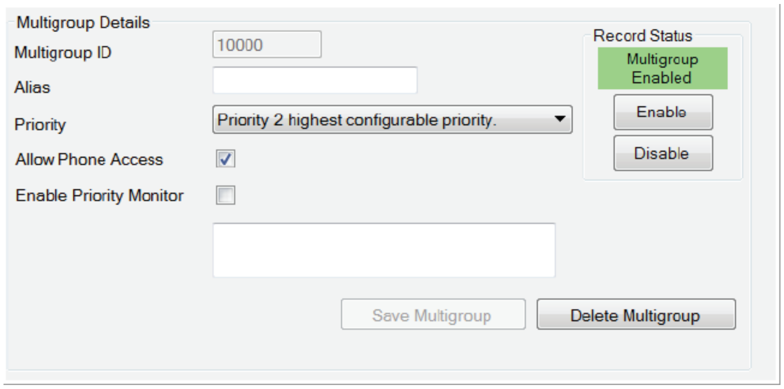
When enabling Priority Monitor for a specific Group ID, the Network Manager may present a warning message, indicating that the Group ID is in conflict in with another Priority Monitor group. This can occur because of the way Priority Announcements are sent over-the-air. The Talk Group ID for a Priority Call is abbreviated if the Group ID number is larger than what can be represented with 18 bits (262,142). Larger Group ID numbers can be used, but are not recommended. If a larger number is sent, its abbreviated format can potentially look the same to a Connect Plus radio as another smaller Priority Monitor Group ID number. This can cause a radio to respond to an announcement that is not for its “true” Priority Monitor Group ID. If this occurs, the radio will **not** unmute to the unexpected Group, but it will miss audio for the group is was monitoring when it decoded the Priority Announcement. The best way to avoid possible Priority Monitor conflicts is to limit all Priority Group ID numbers to 262,142 (or less) wherever possible.

6.1.3.7 Notes

This field allows the user to create a note (alphanumeric string) about the radio, Group or Multigroup. The maximum number of characters is 255.

6.1.4 Multigroup Details

Figure 49: Multigroup Details Screen



Multigroup Details

Multigroup ID: 10000

Alias:

Priority: Priority 2 highest configurable priority.

Allow Phone Access ☑

Enable Priority Monitor ☐

Record Status: Multigroup Enabled

6.1.4.1 Multigroup ID

This parameter defines the Multigroup ID programmed into the Connect Plus Option Board for this radio unit. The XRC automatically provides audio for this ID at any network site where this radio registers. To enter the Multigroup ID for this radio, select the bullet labeled **Use**, and then enter the Multigroup ID in the field to the right. There must already be a Multigroup record that matches this ID in the user database. If this radio does not use a Multigroup ID, select the bullet labeled **None**.

Minimum	1
Maximum	16,776,351
Increment	1
Default	Blank

NOTICE: If a Multigroup ID number is entered that does not conform to the expected Multigroup number format, an exclamation (!) mark in a red circle is displayed next to the field. Pass the cursor over the circle to display the error and an example of a valid Multigroup ID number.

6.1.4.2 Alias

This parameter defines the alphanumeric alias of the MOTOTRBO Subscriber Unit, Group or Multigroup. The maximum number of characters is 255.

6.1.4.3 Record Status

This section displays and enables to change the status of the user record for this Group or Multigroup ID.

Perform one of the following actions:

- Click **Enable** to display the record as Group Enabled (green).
- Click **Disable** to display the record as Group Disabled (red).

NOTICE: There is no over-the-air command sent when the buttons are clicked. The change is enforced the next time a radio user attempts to initiate a call or text using the Group ID or Multigroup ID.

6.1.4.4 Priority

This parameter defines the priority level of the radio, Group or Multigroup ID corresponding to this record. It is used for prioritizing calls in Busy Queue.

The range of the priority level is from 2 to 8: **Priority 2** is the highest, and **Priority 8** is the lowest configurable priority.

6.1.4.5 Allowing Phone Access

Procedure:

Check (enable) this box if a Telephone User should be allowed to access this Group or Multigroup.

6.1.4.6 Priority Monitor

Checking this box enables Priority Monitor announcements for this Multigroup ID.

The Multigroup record should be enabled for Priority Monitor if the corresponding Multigroup ID is configured as a Priority One or Priority Group in any Connect Plus radio throughout the network. When enabling Priority Monitor for a specific Group (or Multigroup) ID, the Network Manager may present a warning message, advising that the Group ID is in conflict in with another Priority Monitor group. This can occur because of the way Priority Announcements are sent over-the-air.

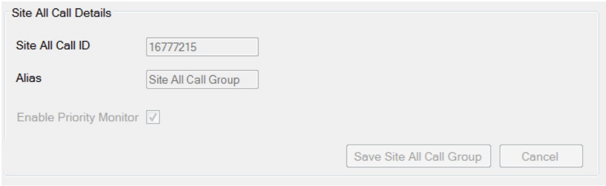
The Talk Group ID for a Priority Call is abbreviated if the Group ID number is larger than what can be represented with 18 bits (262,142). Larger Group ID numbers can be used, but are not recommended. If a larger number is sent, its abbreviated format can potentially look the same to a Connect Plus radio as another smaller Priority Monitor Group ID number. This can cause a radio to respond to an announcement that is not for its “true” Priority Monitor Group ID. If this occurs, the radio will **not** unmute to the unexpected Group, but it will miss audio for the group is was monitoring when it decoded the Priority Announcement. The best way to avoid possible Priority Monitor conflicts is to limit all Priority Group ID numbers to 262,142 (or less) wherever possible.

6.1.4.7 Notes

This field allows the user to create a note (alphanumeric string) about the radio, Group or Multigroup. The maximum number of characters is 255.

6.1.5 Site All Call Details

Figure 50: Site All Call Details Screen



Site All Call Details

Site All Call ID: 16777215

Alias: Site All Call Group

Enable Priority Monitor ☑

Beginning with Connect Plus System Release 1.6, the Network Manager displays a record for the Site All Call ID.

The Site All Call ID group record cannot be deleted, and it cannot be edited.

6.1.5.1 Enabling Priority Monitor

When and where to use: Priority Monitor is always enabled in the Site All Call Details.

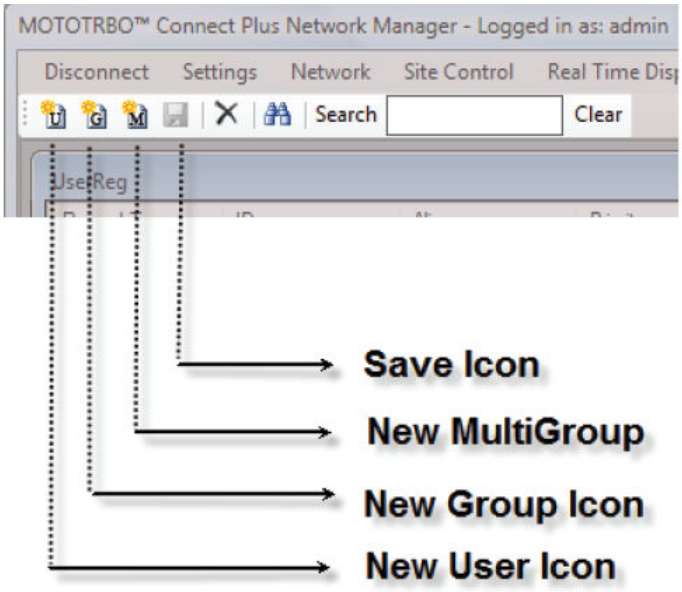
6.1.6 Creating Subscriber/Group/Multigroup Records

The following sections describe ways of creating records using the **Menu Bar** → **Submenu Bar** → **Display Field**.

6.1.6.1 Submenu Bar for Records Creation

The sections which follow explains the steps of creating a new subscriber unit, group and multigroup using the icons within the **Submenu Bar**.

Figure 51: Icons Within the Submenu Bar



6.1.6.1.1 Creating a New Subscriber Unit

Procedure:

1. Select **Settings** → **Users**.
2. Click the **New User** icon on the submenu bar.

   The User Details on the right side of the screen are cleared.
3. Enter Subscriber information.
4. Click **Save** on the submenu bar or **Save User** at the bottom of the **User Details** box to save the record.

6.1.6.1.2
Canceling a New User Record

Procedure:

1 Click outside the **User Details** box.

The following message appears: `There are unsaved changes pending. Would you like to discard these changes and continue?`

2 To discard current changes and continue, click **Yes**.

6.1.6.1.3
Creating a New Group

Procedure:

1 Select **Settings** → **Users**.

2 Click the **New Group** icon on the submenu bar.

3 Enter the Group information.

4 Click the **Save** icon on the submenu bar or the **Save Group** button at the bottom of the Group Details box to save the record.

6.1.6.1.4
Creating a New Multigroup

Procedure:

1 From the Menu Bar, select **Settings** → **Users**.

2 Click **New** from the Multigroup menu bar.

The **Multigroup Details** on the right side of the screen are cleared.

3 Enter the Multigroup information.

4 Click the **Save** on the submenu bar or **Save Multigroup** at the bottom of the **Multigroup Details** box to save the record.

6.1.6.1.5
Canceling A New Group/Multigroup Record

Procedure:

1 Click outside the **Group/Multigroup Details** box.

The following message appears: `There are unsaved changes pending. Would you like to discard these changes and continue?`

2 Click **Yes** to discard current changes and continue.

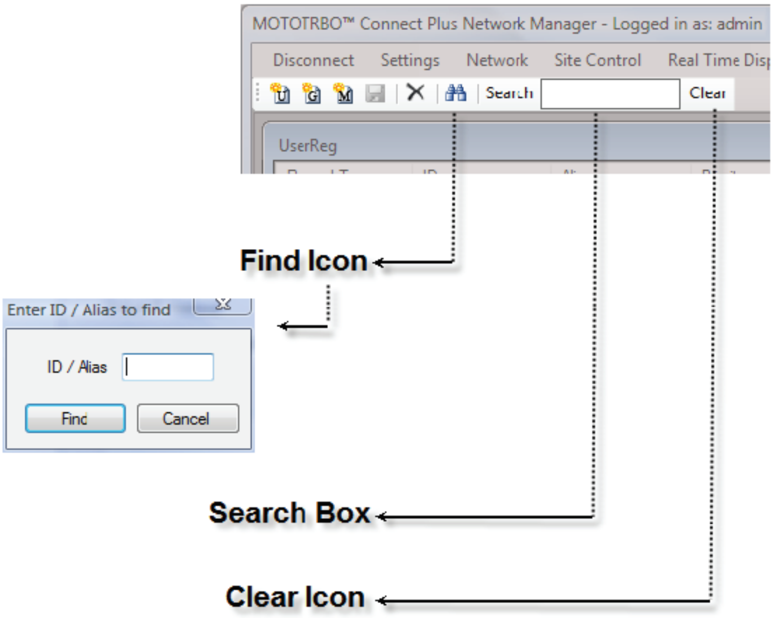
6.1.7
Locating Subscriber/Group/Multigroup Records

The following sections explain ways to search for a subscriber, group or multigroup.

6.1.7.1
Submenu Bar Find Tools

Searching for a Subscriber Unit(s), Group(s), or Multigroup(s) can be done via the Find tool which is accessible from the **Submenu Bar**.

Figure 52: Find Tool in the Submenu Bar



6.1.7.1.1
Searching for the Records

To find a record of a Subscriber Unit(s), Group(s), or Multigroup(s) use either the **Find** icon or a search text box.

Procedure:

1. Select **Settings** → **Users**.
2. Perform one of the following actoins:
   - Click **Find** on the submenu bar. The **Enter ID/Alias to find** dialog box appears.
   - Click inside the **Search Text Box** on the submenu bar.
3. Enter a search string consisting of letters and/or numbers. As you type, the screen displays all records that match the search criteria in the ID, Alias, Status, Serial Number, Multigroup ID or Notes fields.

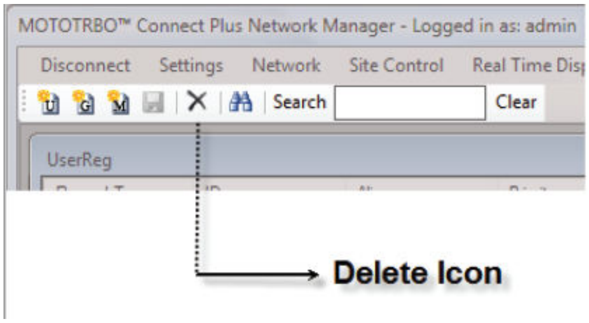
   In order to reduce the number of possible matches, type as much information about the desired record as possible.
4. To clear search results that are displayed in the list, click **Clear** on the submenu bar.

6.1.8
Deleting Subscriber/Group/Multigroup Records

The following topics describe how to delete the subscriber, group and multigroup records.

6.1.8.1
Deleting Records Using the Submenu Bar

Figure 53: Delete Icon in the Submenu Bar



6.1.8.1.1
Deleting a Subscriber Unit

Procedure:

1. Select **Settings** → **Users**.
2. Select the Subscriber Unit to delete.
3. Click **Delete User**.

   A dialog box appears, asking to confirm the deletion.

4. Click **Yes** to delete the record or **No** to keep the record.

6.1.8.1.2
Deleting a Group

Procedure:

1. Select **Settings** → **Users**.
2. Select the Group to delete.
3. Click the **Delete** option.

   A dialog box appears, asking to confirm the deletion.

4. Click **Yes** to delete the record, or **No** to keep the record.

6.1.8.1.3
Deleting a Multigroup

Procedure:

1. Select **Settings** → **Users**.
2. Select the Multigroup to delete.
3. Click the **Delete** option.

   A dialog box appears, asking to confirm the deletion.

4. Click **Yes** to delete the record, or **No** to keep the record.

6.2

Site Access and Permanent Registration

The Site Access and Permanent Registration Screen is used to configure three Connect Plus features: SU Site Restriction, Talk Group Site Restriction, and Permanently Registered Groups of a site.

NOTICE: The **Site Access and Permanent Registration** screen and the **User Registration** screen (**Settings** → **Users**) are both capable of modifying information in the Connect Plus user database. It is not recommended to open both screens at the same time, since edits performed on one screen can cause information displayed on the other screen to become "stale". To assure that a screen is displaying current data, click **Get List** on the **Site Access and Permanent Registration** screen or **Refresh List** on the **User Registration** screen.

SU Site Restriction

The SU Site Restriction feature provides the ability to control which network sites specific subscriber radios can and cannot use. When a subscriber radio is restricted from using a network site, it cannot register on the site, or use the site for any type of call – including Emergency Call or Emergency Alert. The radio must locate an allowed (not restricted) site where it can successfully register and initiate a call. In order for a subscriber radio to learn that it cannot use a network site, it must make at least one attempt to register with the site. The controller responds to the registration by telling the radio that it cannot use the site, which causes the radio to go back into search and to look for a different site. The radio also places the site on an internal “blacklist” and will not send any subsequent registration attempts to the site as long as it remains on the internal blacklist. The site blacklist is cleared when the radio resets for any reason, such as power cycle or codeplug programming. By default, all radios are allowed to use all network sites. The Site Access and Permanent Registration screen provides two ways to configure restricted sites for subscriber units:

- From the site perspective view, the application user can add or remove one or more radios from the list of restricted radios of the site. Any valid subscriber that is not on the restricted list is allowed to use the site.
- From the SU perspective view, the application user can add or remove one or more restricted sites for a specific subscriber radio.

Talk Group Site Restriction

The Talk Group Site Restriction feature provides the ability to control which network sites can and cannot be used by a specific Talk Group ID. If a subscriber attempts to register with a network site while selected to a Talk Group ID which is restricted for that site, the radio cannot register on the site while selected to the restricted group unless the radio is in “Emergency Pending” state. Otherwise, the radio must locate a site where the Talk Group is not restricted, or the radio user must change the channel selector to select a Talk Group that is not restricted at the site. In order to learn that a Talk Group is not allowed (restricted) at a site, the radio must make at least one attempt to register with the site while selected to the restricted Talk Group. The controller responds to the registration by telling the radio that its selected Talk Group cannot use the site, which causes the radio to go back into search and to look for a different site. The radio also places the site on an internal, Talk Group specific, “blacklist” and will not send any subsequent registration attempts to the site while selected to that Talk Group as long as the site/group combination remains on the internal blacklist. The blacklist is cleared under various circumstances described in the *MOTOTRBO Connect Plus System Planner*. By default, all Talk Groups are allowed to use all network sites. The **Site Access and Permanent Registration** screen provides two ways to configure restricted sites for Talk Group IDs:

- From the site perspective view, the application user can add or remove one or more Talk Groups from the list of restricted Talk Groups of a site. Any valid Talk Group that is not on the restricted list is allowed to use the site.
- From the Talk Group perspective view, the application user can add or remove one or more restricted sites for a specific Talk Group ID.

- The following configuration rules pertain to Talk Group site restriction:
  - The same Talk Group cannot be on both the restricted list and the permanently registered list for the same site. The features are mutually exclusive.
  - Site All Call ID cannot be restricted at any site.

NOTICE: If radios are currently registered to a site when the status of their selected Talk Group is changed from `Allowed` to `Restricted` for that site, voice calls and text messages targeting the newly restricted Group may continue to be transmitted at the site until all of the impacted radios have registered to a different site, or re-registered with the same site on a different Talk Group, or deregistered from the network. For more important information on this feature, please see the *MOTOTRBO Connect Plus System Planner*.

Permanently Registered Talk Groups

The Permanent Talk Group Registration feature can be utilized to enhance network scan operation by configuring a list of Talk Groups that should remain permanently registered to a Connect Plus site. When a Group is permanently registered, and when the Group is active elsewhere in the network, the local site controller transmits audio for the group (subject to repeater resource availability), even when there no radio at the site that is registered to the Group. This increases the chances that a scanning radio can hear transmissions for its scan list groups (when the listening radio is not at the same site where the transmission originates). Permanent Talk Group Registration can be expected to increase the number of calls that a site transmits when compared to the default system operation (which is to only transmit audio when at least one radio is registered to the Group). “Busy” conditions (requiring a wait in the Busy Queue) will be more frequent than at sites that do not have permanently registered groups. Also, IP bandwidth between sites must be sufficient to handle the networked calls triggered by the permanent Talk Group registration feature. The **Site Access and Permanent Registration** screen provides two ways to configure permanently registered sites for Talk Group IDs:

- From the site perspective view, the application user can add or remove one or more Talk Groups from the list of permanently registered Talk Groups of the site.
- From the Talk Group perspective view, the application user can add or remove one or more permanently registered sites for a specific Talk Group ID.
- The following configuration rules pertain to Talk Group permanent registration by site:
  - The same Talk Group cannot be on both the restricted list and the permanently registered list for the same site. The features are mutually exclusive.
  - Site All Call ID cannot be configured as a permanently registered group. This is unnecessary because radio-initiated site all call transmissions are always carried on the originating site, but are not networked to other sites.
  - Multigroups cannot be configured as permanently registered. This is unnecessary because the controller automatically registers multigroup of the radio on behalf of the radio, even if the radio is not physically selected to its Multigroup ID.
  - The number of permanently registered groups that are configured for any specific site cannot be greater than 100.

6.2.1 Launching the Site Access and Permanent Registration Screen

Procedure:

From the Menu Bar, select **Settings** → **Site Access and Permanent Registration**.

The **Site Access and Permanent Registration** screen launches with the Site bullet selected by default.

6.2.2 Entering IDs

There are several ways to enter IDs into the **Changes to List** field. This methods apply to Subscriber IDs, Group IDs and Site IDs.

Procedure:

You can enter IDs by using one of the following methods:

- Enter the ID, or a comma separated list of IDs.
- Enter a range expression of IDs by using a hyphen between the two IDs at either end of the range.
  A combination of comma separated IDs and range expressions are acceptable, provided that all IDs explicitly or implicitly listed in the Changes to List field are actual IDs in the user database (or Site IDs in the Multisite Table) and the total of all IDs explicitly or implicitly listed cannot be greater than 100.
- Paste IDs from the Windows clipboard, provided that the total number and expressions follow the above rules.
- If selecting IDs to remove from the Current List, an alternative method to enter the IDs is to select (or multi-select) one or more IDs from the Current List.

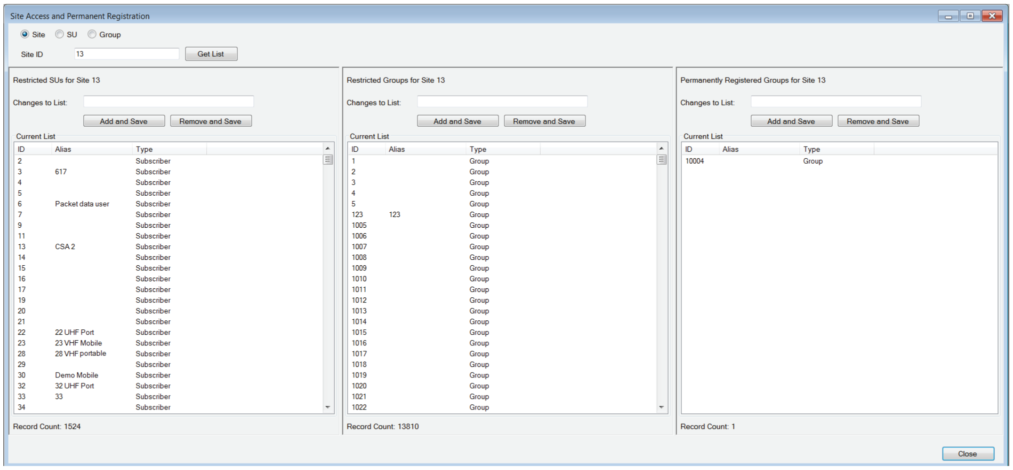
6.2.3 Configuring a List of Restricted Radios (SUs) for a Specific Site

Procedure:

1. Launch the **Site Access and Permanent Registration** Screen.
2. Click **Site bullet** (if not already selected).
3. Enter the site number to be configured into the **Site ID** field.

   The entered site number must be a valid XRC Controller site number in the Multisite Table of the connected site.
4. Press the **Get List** button.

   The application retrieves three lists; Restricted SUs, Restricted Groups and Permanently Registered Groups. The lists are displayed in three panels, as shown in the following image. In the panel labeled, **Restricted SUs for Site n** (where <*n*>=Site ID entered in step 3), the Current List contains a list of currently restricted Radio IDs (if any), along with Aliases (if any) for the restricted IDs.



Site Access and Permanent Registration

● Site ○ SU ○ Group

Site ID: 13

Restricted SUs for Site 13

Changes to List:

Current List

ID	Alias	Type
2		Subscriber
3	617	Subscriber
4		Subscriber
5		Subscriber
6	Packet data user	Subscriber
7		Subscriber
9		Subscriber
11		Subscriber
13	CSA 2	Subscriber
14		Subscriber
15		Subscriber
16		Subscriber
17		Subscriber
19		Subscriber
20		Subscriber
21		Subscriber
22	22 UHF Port	Subscriber
23	23 VHF Mobile	Subscriber
28	28 VHF portable	Subscriber
29		Subscriber
30	Demo Mobile	Subscriber
32	32 UHF Port	Subscriber
33	33	Subscriber
34		Subscriber

Record Count: 1524

Restricted Groups for Site 13

Changes to List:

Current List

ID	Alias	Type
1		Group
2		Group
3		Group
4		Group
5		Group
123	123	Group
1005		Group
1006		Group
1007		Group
1008		Group
1009		Group
1010		Group
1011		Group
1012		Group
1013		Group
1014		Group
1015		Group
1016		Group
1017		Group
1018		Group
1019		Group
1020		Group
1021		Group
1022		Group

Record Count: 13810

Permanently Registered Groups for Site 13

Changes to List:

Current List

ID	Alias	Type
10004		Group

Record Count: 1

5. Enter one or more `Subscriber Unit IDs` (also called Radio IDs) into the Changes to List field for Restricted SUs. There are several ways to enter the SUIDs as discussed in Entering IDs on page 135.

   Any ID that is entered into the **Changes to List** field must accurately represent a Subscriber ID in the Connect Plus User Registry. This includes SUIDs that are inferred within range expressions. The application accepts up to 100 SUIDs for a single change. If more are needed, this can be accomplished by making multiple changes.
6. Enter the SUIDs to change into **Changes to List**.
7. Perform one of the following actions:
   - Click **Add and Save** to add the Group IDs to the Current List.
   - Click **Remove and Save**to remove the Group IDs from the Current List.

   The system checks and validates the submitted changes. After validating the changes, the application updates the Current List if all changes are accepted, or responds with an appropriate error indication for the first rejected change (due to the validation check). Normally all changes must be accepted for any change to be accepted. If the application displays a red circle with an exclamation point icon, then place the pointer arrow over the icon for more information. Investigate any error message, resolve the issue, and then try again.

6.2.4
Configuring a List of Restricted Talk Groups for a Specific Site

Procedure:

1. Launch the **Site Access and Permanent Registration** screen.
2. Click **Site bullet** (if not already selected).
3. Enter the site number to be configured into the Site ID field.

   The entered site number must be a valid XRC Controller site number in the Multisite Table of the connected site.
4. Press the **Get List** button.

   The application retrieves three lists; Restricted SUs, Restricted Groups, and Permanently Registered Groups. In the panel labeled **Restricted Groups for Site n** (where ***<n>***=Site ID entered in step 3), the Current List contains a list of currently restricted Group IDs (if any), along with Aliases (if any) for the restricted IDs.
5. Enter one or more Group IDs into the **Changes to List** field for Restricted Groups.

   This includes Group IDs that are inferred within range expressions. The application accepts up to 100 Group IDs for a single change. If more are needed, this can be accomplished by making multiple changes.
6. Enter the Group IDs to change into **Changes to List**.
7. Perform one of the following actions:
   - Click **Add and Save** to add the Group IDs to the Current List.
   - Click **Remove and Save**to remove the Group IDs from the Current List.

The system checks and validates the submitted changes. After validating the changes, the application updates the Current List if all changes are accepted, or responds with an appropriate error indication for the first rejected change (due to the validation check). Normally all changes must be accepted for any change to be accepted. If the application displays a red circle with an exclamation point icon, then place the pointer arrow over the icon for more information. Investigate any error message, resolve the issue, and then try again.

6.2.5 Configuring a List of Permanently Registered Talk Groups for a Specific Site

Procedure:

1. Launch the **Site Access and Permanent Registration** screen.
2. Click on **Site** bullet (if not already selected).
3. Enter the site number to be configured into the **Site ID** field.

   The entered site number must be a valid XRC Controller site number in the Multisite Table of the connected site.
4. Press the **Get List** button.

   The application retrieves three lists; Restricted SUs, Restricted Groups and Permanently Registered Groups. In the panel labeled, **Permanently Registered Groups for Site n** (where ***<n>***=Site ID entered in step 3), the Current List contains a list of permanently registered Group IDs (if any), along with Aliases (if any) for the permanently registered IDs.
5. Enter one or more Group IDs into the **Changes to List** field for Permanently Registered Groups.

   Any ID that is entered into the **Changes to List** field must accurately represent a Group ID in the Connect Plus User Registry. This includes Group IDs that are inferred within range expressions. The application will accept up to 100 Group IDs for a single change. If more are needed, this can be accomplished by making multiple changes.
6. Enter the Group IDs to change into **Changes to List**.
7. Perform one of the following actions:
   - Click **Add and Save** to add the Group IDs to the Current List.
   - Click **Remove and Save**to remove the Group IDs from the Current List.

The system checks and validates the submitted changes. After validating the changes, the application updates the Current List if all changes are accepted, or responds with an appropriate error indication for the first rejected change (due to the validation check). Normally all changes must be accepted for any change to be accepted. If the application displays a red circle with an exclamation point icon, then place the pointer arrow over the icon for more information. Investigate any error message, resolve the issue, and then try again.

6.2.6 Configuring a List of Restricted Sites for a Specific Radio

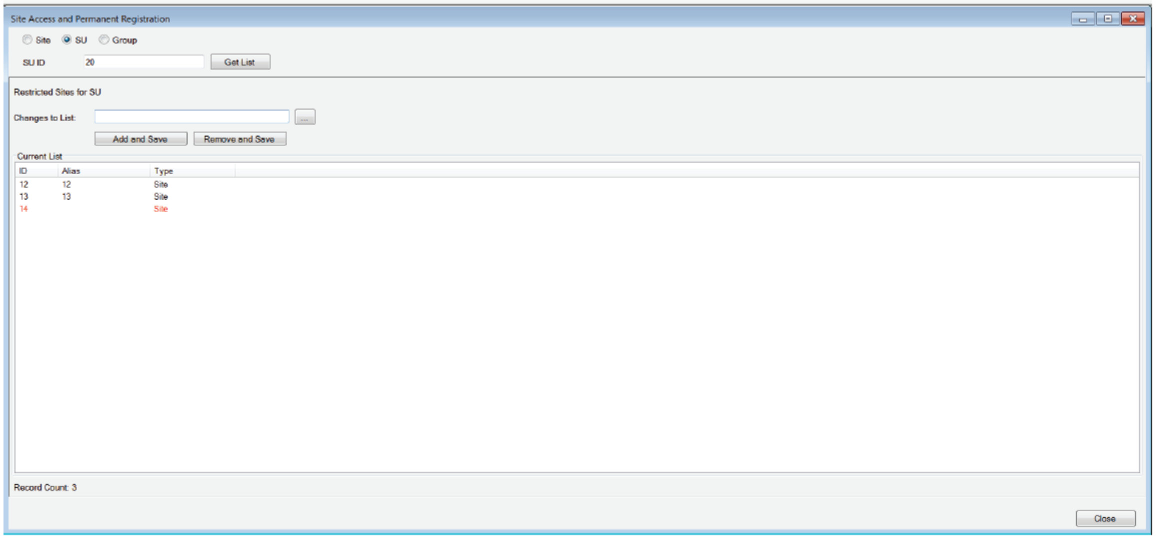
Procedure:

1. Launch the **Site Access and Permanent Registration** screen.
2. Click **SU** bullet (if not already selected).
3. Enter the SUID to be configured into the **SU ID** field.

   The entered site SUID must be an actual Subscriber Unit ID (Radio ID) in the Connect Plus user database.
4. Press the **Get List** button.

   The application retrieves a list of currently restricted sites for the radio and populates the **Current List** with the currently restricted sites. The Current List contains a list of currently restricted Site IDs (if any), along with Aliases (if any) for the Site IDs. If any Site ID displays in red text in the Current List, this indicates the Site ID is not listed on the Multisite Table of the connected site.

Figure 54: Current List



○ Site ● SU ○ Group

SU ID: 20

Restricted Sites for SU

Changes to List:

Current List

ID	Alias	Type
12	12	Site
13	13	Site
14		Site

Record Count: 3

5 Enter one or more Site IDs into the **Changes to List** field for restricted sites by following one of the following methods:

- Follow the steps in Entering IDs on page 135.
- Click the ... button to launch the **Site Selector** window.
  - In the **Site Selector**, check all Site Numbers that you would like to enter into the **Changes to List** field.
  - When ready, press the **Apply** button on the **Site Selector.** The selected Site IDs is automatically placed into the **Changes to List** field, replacing any data that may have been previously entered into the field, and the Site Selector closes.

Any ID that is entered into the **Changes to List** field must accurately represent an XRC Controller Site ID in the Multisite Table of the connected site. This includes Site IDs that are inferred within range expressions.

6 Enter the Site IDs to change into **Changes to List**.

7 Perform one of the following actions:

- Click **Add and Save** to add the Site IDs to the Current List.
- Click **Remove and Save**to remove the Site IDs from the Current List.

The system checks and validates the submitted changes. After validating the changes, the application updates the Current List if all changes are accepted, or responds with an appropriate error indication for the first rejected change (due to the validation check). Normally all changes must be accepted for any change to be accepted. If the application displays a red circle with an exclamation point icon, then place the pointer arrow over the icon for more information. Investigate any error message, resolve the issue, and then try again.

6.2.7 Configuring a List of Restricted Sites for a Specific Talk Group ID

Procedure:

1 Launch the **Site Access and Permanent Registration** screen.

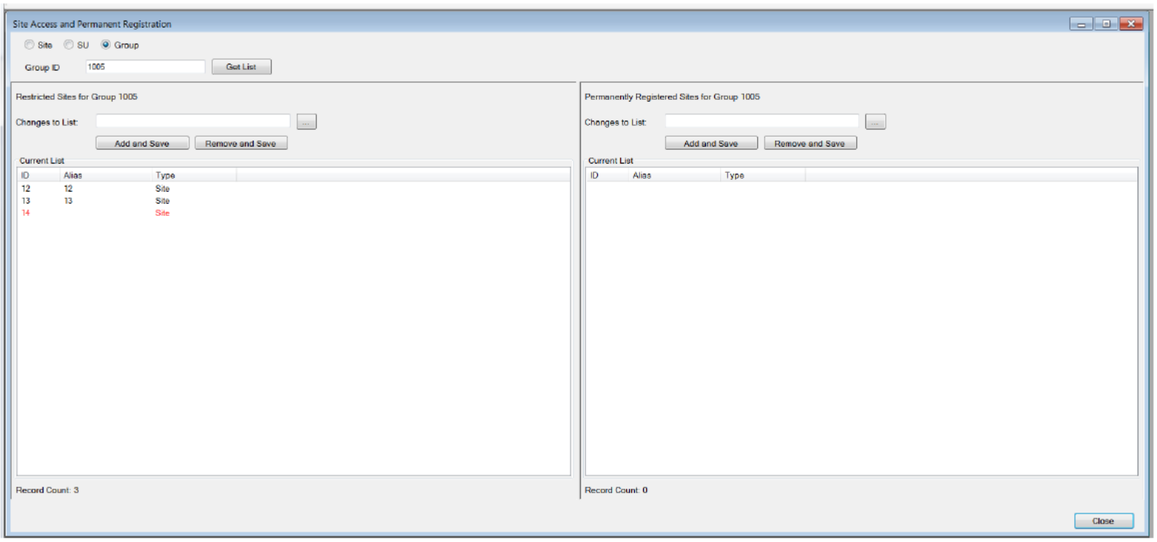
2 Click on **Group** bullet (if not already selected).

3 Enter the Group ID to be configured into the **Group ID** field.

The entered Group ID must be an actual Talk Group ID in the Connect Plus user database.

4 Press the **Get List** button.

The application retrieves two lists; a list of restricted sites for this Group ID and a list of permanently registered sites for this Group ID. The lists are displayed in two panels, as shown in the following image. In the panel labeled **Restricted Sites for Group n** (where <*n*>=Group ID entered in step 3), the Current List contains a list of currently restricted Site IDs (if any), along with Aliases (if any) for the Site IDs. If any Site ID displays in red text in the Current List, this indicates the Site ID is not listed on the Multisite Table of the connected site.



Site Access and Permanent Registration

○ Site ○ SU ● Group

Group ID 1005

Restricted Sites for Group 1005

Changes to List:

Current List

ID	Alias	Type
12	12	Site
13	13	Site
14		Site

Record Count: 3

Permanently Registered Sites for Group 1005

Changes to List:

Current List

ID	Alias	Type

Record Count: 0

5 Enter one or more Site IDs into the **Changes to List** field for restricted sites by one following of the following methods:

- Follow the steps in Entering IDs on page 135.
- Click the ... button to launch the **Site Selector** window.
  - In the **Site Selector**, check all Site Numbers that you would like to enter into the **Changes to List** field.
  - When ready, press the **Apply** button on the **Site Selector.** The selected Site IDs is automatically placed into the **Changes to List** field, replacing any data that may have been previously entered into the field, and the Site Selector closes.

Any ID that is entered into the **Changes to List** field must accurately represent an XRC Controller Site ID in the Multisite Table of the connected site. This includes Site IDs that are inferred within range expressions.

6 Enter the Site IDs to change into **Changes to List**.

7 Perform one of the following actions:

- Click **Add and Save** to add the Site IDs to the Current List.
- Click **Remove and Save**to remove the Site IDs from the Current List.

The system checks and validates the submitted changes. After validating the changes, the application updates the Current List if all changes are accepted, or responds with an appropriate error indication for the first rejected change (due to the validation check). Normally all changes must be accepted for any change to be accepted. If the application displays a red circle with an exclamation point icon, then place the pointer arrow over the icon for more information. Investigate any error message, resolve the issue, and then try again.

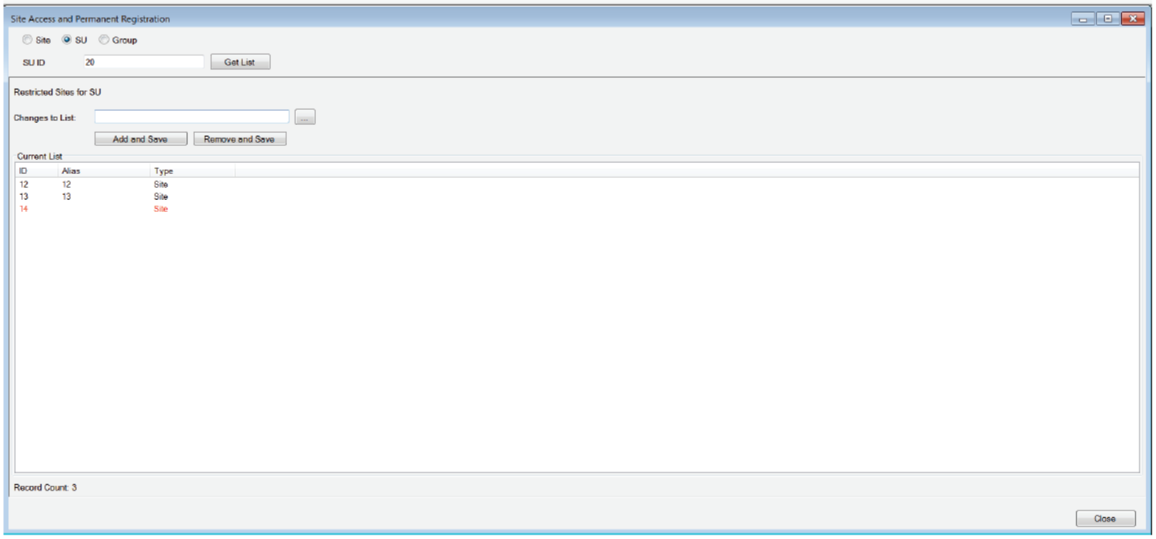
6.2.8 Configuring a List of Permanently Registered Sites for a Specific Talk Group ID

Procedure:

1. Launch the **Site Access and Permanent Registration** screen.
2. Click on **Group** bullet (if not already selected).
3. Enter the Group ID to be configured into the **Group ID** field.

   The entered Group ID must be an actual Talk Group ID in the Connect Plus user database.
4. Press the **Get List** button.

   The application retrieves two lists; a list of restricted sites for this Group ID and a list of permanently registered sites for this Group ID. In the panel labeled, “Permanently Registered Sites for Group n (where n=Group ID entered in Step 3), the Current List contains a list of Site IDs (if any) where this Group is permanently registered, along with Aliases (if any) for the Site IDs. If any Site ID displays in red text in the Current List, this indicates the Site ID is not listed on the Multisite Table of the connected site.

   Site Access and Permanent Registration

   ○ Site ● SU ○ Group

   SU ID 20

   Restricted Sites for SU

   Changes to List:

   Current List

ID	Alias	Type
12	12	Site
13	13	Site
14		Site

   Record Count: 3

5. Enter one or more Site IDs into the **Changes to List** field for permanently registered sites by following one of the following methods:
   - Follow the steps in Entering IDs on page 135.
   - Click the ... button to launch the **Site Selector** window.
     - In the **Site Selector**, check all Site Numbers that you would like to enter into the **Changes to List** field.
     - When ready, press the **Apply** button on the **Site Selector.** The selected Site IDs is automatically placed into the **Changes to List** field, replacing any data that may have been previously entered into the field, and the Site Selector closes.

   Any ID that is entered into the Changes to List field must accurately represent a XRC Controller Site ID in the Multisite Table of the connected site. This includes Site IDs that are inferred within range expressions.
6. Enter the Site IDs to change into **Changes to List**.
7. Perform one of the following actions:

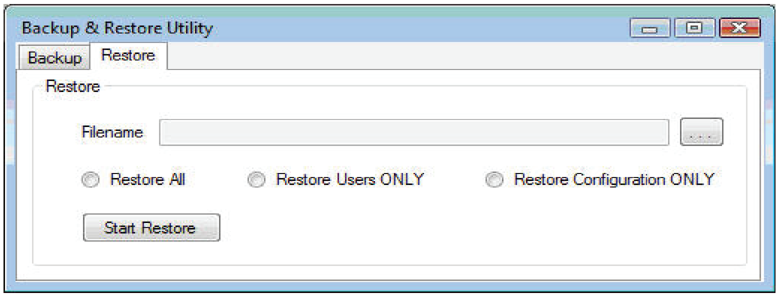
- Click **Add and Save** to add the Site IDs to the Current List.
- Click **Remove and Save**to remove the Site IDs from the Current List.

The system checks and validates the submitted changes. After validating the changes, the application updates the Current List if all changes are accepted, or responds with an appropriate error indication for the first rejected change (due to the validation check). Normally all changes must be accepted for any change to be accepted. If the application displays a red circle with an exclamation point icon, then place the pointer arrow over the icon for more information. Investigate any error message, resolve the issue, and then try again.

6.3 Backup/Restore Utility

This option allows creating a site backup file containing Network Settings, Site Configuration, Multisite Configuration, Alerts/Alarms configuration, SMTP configuration, Users, Groups, and Multigroups.

Figure 55: Backup and Restore Utility Window



The Restore tab provides three options. Only one option can be selected at a time.

Restore All

The settings from the uploaded file will replace the current site configuration and user database of the device.

Restore Users Only

The user database from the uploaded file will replace the current user database of the device. Other configurable settings for the device are not changed.

Restore Users should only be used when there is not any other XRC or XRT device attached to the network that has a copy of the user database. If there is another XRC or XRT device attached to the network, the user records will be synchronized automatically.

Restore Configuration Only

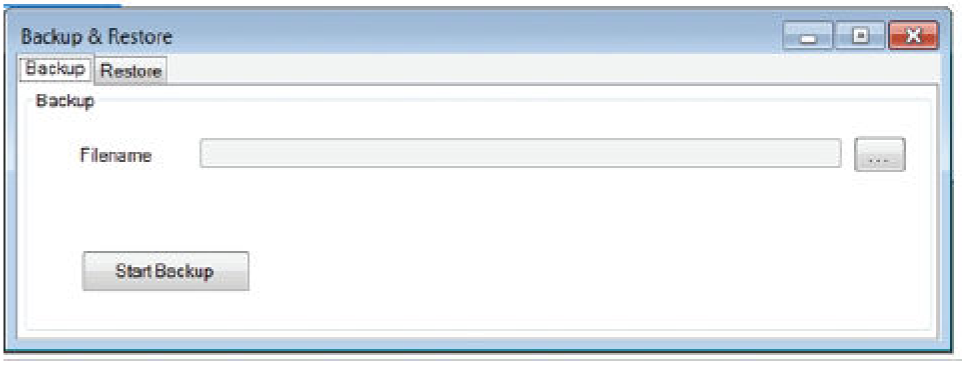
The settings from the uploaded file will replace all configurable settings for the device except for the user database. The current user database of the device is not changed.

6.3.1 Saving a Site Configuration to a File

Procedure:

1 From the Menu Bar, select **Settings** → **Backup & Restore Utility**.

The **Backup & Restore** screen appears.



2 Open the **Backup** tab.

3 Click on the **Browse** icon, select the location to save the site configuration to and click **Save**.

4 Click on the **Start Backup** button.

The message `Backup completed successfully!` appears next to the **Start Backup** button.

6.3.2 Restore Tab

The Restore tab provides three options: **Restore All**, **Restore Users ONLY**, and **Restore Configuration Only**.

Procedure:

Choose one of the following options for restoring a site configuration:

- **Restore All**

The settings and user database from the uploaded file replaces the current site configuration and user database of the device.

- **Restore Users Only**

The user database from the uploaded file replaces the current user database of the device. Other configurable settings for the device are not changed.

Restore Users should only be used when there is not any other XRC or XRT device attached to the network that has a copy of the user database. If there is another XRC or XRT device attached to the network, the user records will be synchronized automatically.

- **Restore Configuration Only**

The settings from the uploaded file replace all configurable settings for the device, except for the user database. The current user database of the device is not changed.

6.3.2.1 Restoring a Site Configuration from a File

Procedure:

1. From the Menu Bar, select **Settings** → **Backup & Restore Utility**.

   The **Backup & Restore** screen appears.

2. Open the **Restore** tab.
3. Click the **Browse** icon, select the file to be restored and click **Open**.
4. Click a bullet to show which parts of the backup information should be uploaded.
5. Click the **Start Restore** button.

   A message appears, asking to confirm restoration and reboot.

6. Click **Yes** to restore or **No** or **Cancel** to stop the restore.

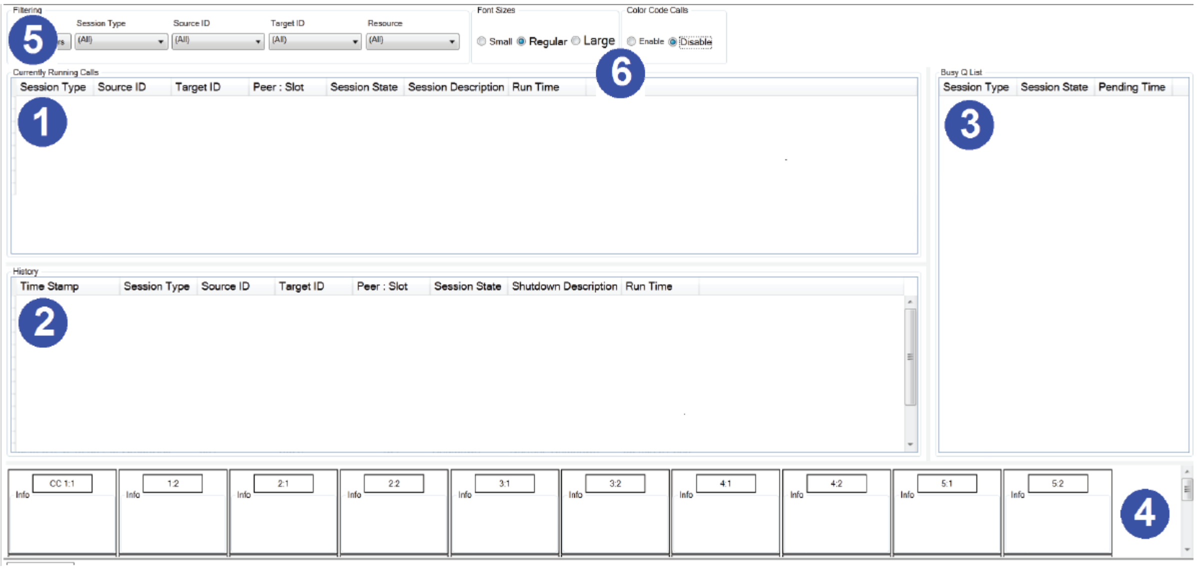
   A message appears under the **Start Restore** button along with a progress bar: `File restore completed successfully! Rebooting...`

6.4 Monitoring Over-the-Air Activity

6.4.1 Real Time Display

The Real Time Display provides information about calls that are presently occurring on the site (Currently Running Calls panel), calls that have recently occurred on the site (History panel), and calls that are queued to occur on the site once a resource becomes available (Busy Q List Panel).

Figure 56: Real Time Display Window



1. Currently Running Panel
2. History Panel
3. Busy Queue Panel
4. Time Slot Area

5 Filters

6 Set Font Size and Enable/Disable Color Coding for Calls

The bottom panel provides a time slot-by-time slot view of site activity. It shows either the current call for each time slot, or if no call is presently occurring, a blank field. The Control Channel (CC) time slot displays current activity, or if there is no current activity, then it displays the last activity. When Color Coding for Calls is enabled, the following colors are used:

- Green for Active Sessions
- Orange for Emergency
- Red for Session Failed or encountered error

Information available on the Real Time Display (RTD) includes the following:

- The type of call (or "session")
- The current state of the call (or "session")
- Who started the call (Source ID)? This is always an individual ID.
- Who was the called party (Target ID)? This can be an individual ID or a Group ID.
- When the call took place (Time Stamp)
- What repeater and slot is (or was) used? (2:1 indicates peer repeater 2, first time slot)

When a session is over, it moves from the Currently Running Calls panel to the History Panel. If the Real Time Display is left open for a long time, the large number of sessions in the History Panel can be detrimental to PC performance due to the memory required to retain the information. If the user desires the historical data about call activity, it is better to download the Air Time Logging records rather than leaving the Real Time Display open for an extended period of time. Session History is limited to 1000 records. When the 1000 record limit is reached, the oldest records are dropped as new records are added.

NOTICE: The Time Slot Area shows which repeater time slots are currently serving as Fast GPS Report Channels (if any). The Real Time Display does not contain any additional data about Fast GPS Channels or Reports. This information is available on the Fast GPS Tracking Window.

6.4.1.1 Call History Details

The **Call Event Detail** window is launched by double-clicking the event on the **History** panel.

The format is as follows:

- Date Stamp
- Time Stamp
- Session Type (Call Type)
- Source ID
- Target ID
- Session State
- Peer Slot
- Description

On a busy site, the **History** panel list scrolls rapidly, and it can be difficult to read the details of individual sessions. To pause the automatic scrolling, right-click the history panel and select one of the following choices:

Pause All

Causes updates to **History** panel to pause until the option is deselected again.

Pause Updates on Mouse Enter

Updates are paused while the mouse pointer is held over the **History** panel. If the mouse pointer is moved away from the **History** panel, the updates resume.

6.5 Site Control

6.5.1 Rebooting a Site

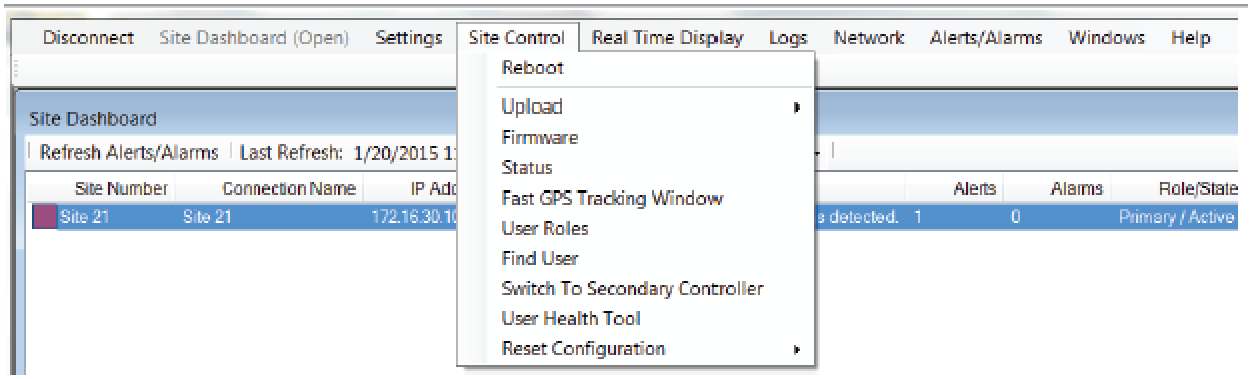
When and where to use:

⚠ **CAUTION:** Rebooting an operational device has a significant impact on site operations. If a reboot must occur, it should be done at a time that will have the least possible impact on site operation (if possible). The following is a partial list of what occurs when a site reboots:

- All Network Manager sessions are disconnected from the site.
- Radios that were using the site go into Search. In a multisite network with overlapping site coverage, these radios may acquire another site. If no other site is available, these radios will need to re-register with this site after it has fully reset and the repeaters have checked back in. The length of time required to re-register all units depends on several factors, such as the number of radios, and how many calls are active on the site.
- Radios that were using the site go into Search. In a multisite network with overlapping site coverage, these radios may acquire another site. If no other site is available, these radios will need to re-register with this site after it has fully reset and the repeaters have checked back in. The length of time required to re-register all units depends on several factors, such as the number of radios, and how many calls are active on the site.
- Site information that has not been saved to permanent memory is lost.

Procedure:

1 From the Menu Bar, select **Site Control** → **Reboot**.



A warning dialog box appears, asking to confirm the reboot.

2 Select one of the following:

- Click **Yes** to reboot.
- Click **No** or **Cancel** to stop the reboot.

6.5.2 Over-the-Air (OTA) File Transfer

Connect Plus allows Over-the-Air (OTA) File Transfer (between the Controller and the Connect Plus SU) for three types of files:

- Option Board Codeplug file (*.efc)
- Network Frequency file (*.tfn)
- Option Board firmware file (*.tfo, *.efo, *.efb)

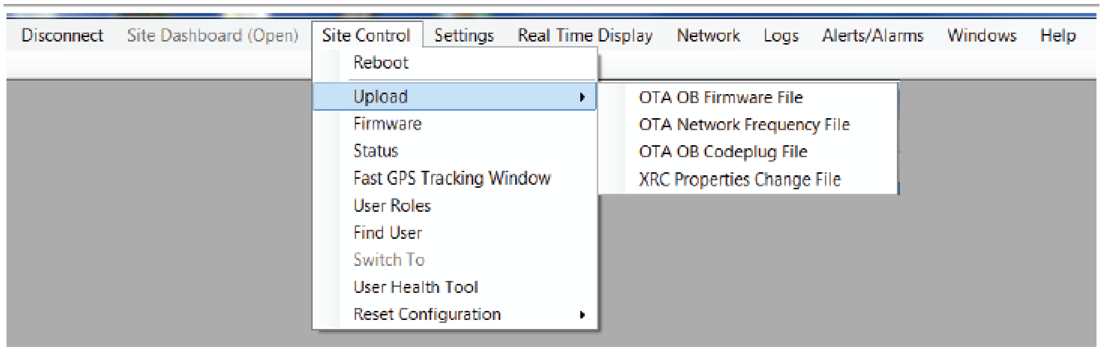
The OTA File Transfer screens are used to select a file for uploading to the XRC. All three screens require the user to browse to and select the desired file. In addition, the OTA OB Firmware File and OTA Network Frequency File screens provide parameters that must be configured prior to uploading the file.

Before utilizing this feature, it is very important for the System Administrator to understand how OTA File transfer functions, how it affects the operation of the Connect Plus SU, and the optimal times and conditions for scheduling OTA File Transfers. For more information on these and other related topics, see the *MOTOTRBO System Planner for Connect Plus*.

6.5.2.1 Uploading Files for OTA File Transfer

Procedure:

1 From the **Site Control** menu, choose the **Upload** option.

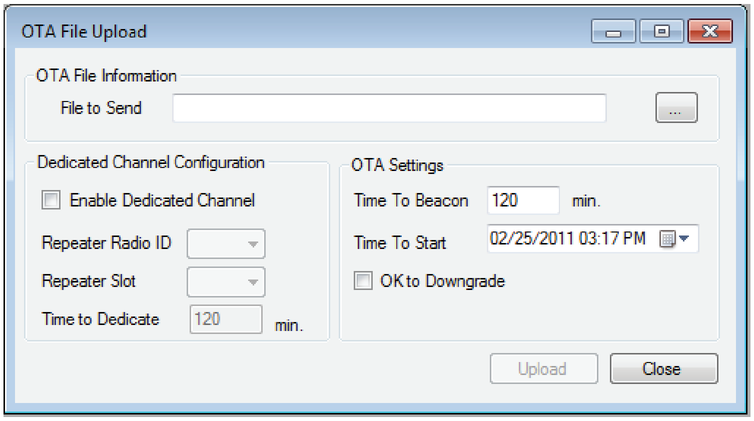


2 Select the OTA File from the submenu.

3 Click the **Browse** icon.

4 Select the file to be loaded and click **Open.**

The OTA File Upload window appears.


OTA File Upload

OTA File Information

File to Send

Dedicated Channel Configuration

□ Enable Dedicated Channel

Repeater Radio ID

Repeater Slot

Time to Dedicate 120 min.

OTA Settings

Time To Beacon 120 min.

Time To Start 02/25/2011 03:17 PM

□ OK to Downgrade

5 Once the rest of the screen has been completed click the **Upload** button to send the file to the XRC.

If the upload is successful then the following message is displayed: File successfully queued for OTA transfer.

6 Click **OK** to close the dialog box.

6.5.2.1.1 OTA Transfer: Option Board Firmware File and Network Frequency File

OTA transfer of the Option Board Firmware File and the Network Frequency file are "Beaconed" file transfers. The availability of these file types is beaconed on the control channel and all subscriber radios that determine that they need the file will join the transfer. After selecting either "OTA OB Firmware File" or "OTA Network Frequency File" from the upload menu, the next step is to select the specific "file to send". After selecting the file to send, there are some additional fields to configure. Configure these settings prior to uploading the selected file to the XRC.

NOTICE: The XRC processes one Beaconed File Transfer (Option Board Firmware File or Network Frequency File) at a time. Do not upload a second file of either type until the XRC has either transmitted or deleted (in the case where it cannot transmit or finish transmitting) any previously uploaded file.

6.5.2.1.1.1 Time to Beacon

This parameter determines how long the XRC "beacons" a special control channel message to inform radios of the file availability.

This time must be equal to the Time to Dedicate.

A setting of 65,535 minutes informs the XRC that the Beacon message should never expire.

Maximum	65,535 mins
Minimum	1 (for .tfn file) 60 (for .tfo, .efo, or .efb file)
Increment	1 min
Default	120 mins

6.5.2.1.1.2 Time to Start

This parameter informs the XRC when to start sending the File Beacon message. The XRC also starts the dedicated channel file transfer at this date and time. Enter a date and time by typing over the current information.

As a convenience, click the arrow to view a drop-down calendar that can be used to select the desired date. The time can only be entered by typing over the current time. The date and time values configured into **Time to Start** are based on PC local time. When uploading the file to the XRC, the Network Manager converts the configured values to UTC time. The controller then starts the file transfer at the requested UTC date and time according to the controller's internal clock. The PC used to upload the file must be in synch with the XRC in regards to UTC time. If they are not in synch, the file transfer may start at a different time than is expected by the Network Manager user. If the configured time is in the past according to the controller's clock, the file transfer will not take place at all. In order for the PC and the XRC to be in synch, both of the following must be true:

1. The PC date and time must be correct for the Time Zone that is configured on the Microsoft Window's Date and Time Properties screen, and
2. The XRC clock must have the correct date and time in UTC. The controller's date and time in UTC can be checked with the Network Manager. (**Settings** → **Date and Time**).

6.5.2.1.1.3 File to Send

This parameter defines the file to be uploaded to the XRC for the Beaconed File Transfer.

File Type	File Extension
Network Frequency File	.tfn
Option Board firmware	.tfo, .efo, .efb

6.5.2.1.1.4 OK to Downgrade

When **OK to Downgrade** is unchecked, the Connect Plus Option Board only acquires files over-the-air that are higher (newer) in version than its current file. This is a recommended operation.

However, there may be special circumstances that require the Option Board to acquire a file that has a lower (older) version number than its current file. When **OK to Downgrade** is checked, the XRC sets a bit in the File Beacon message telling the Connect Plus Option Board that it is OK to downgrade to this file from a higher (newer) version.

NOTICE: The Option Board is coded with certain rules that take precedence over this check box.

6.5.2.1.1.5 Enabling Dedicated Channel

Procedure:

Check this box when a dedicated channel file transfer is desired. This is the only type of OTA File Transfer currently supported.

Values must be entered into all three fields.

The software activates the following fields:

- **Repeater Radio ID**

- **Repeater Slot**
- **Time to Dedicate**

6.5.2.1.1.6
Repeater Radio ID

This parameter defines the Radio ID of the repeater that is used for the dedicated channel transfer.

Minimum	1
Maximum	15
Increment	1
Default	Blank

6.5.2.1.1.7
Repeater Slot

This parameter defines the Repeater Slot of the trunk-to time slot that is used for the dedicated channel transfer.

Minimum	1
Maximum	2
Increment	1
Default	Blank

IMPORTANT: The Control Channel time slot cannot be used.

6.5.2.1.1.8
Time to Dedicate

This parameter determines how long the repeater and time slot are used for the dedicated channel file transfer. During this time, the time slot cannot be used for other calls. Radios may join or leave the dedicated channel transfer at various times (the radio user can cancel out of the transfer by requesting a call).

A setting of 65,535 minutes informs the XRC that the dedicated channel transfer should never expire.

IMPORTANT: Time to Beacon must be equal to **Time to Dedicate**.

Minimum	1 (for .tfn file) 60 (for .tfo, .efo, or .efb file)
Maximum	65,535 mins
Increment	1 min
Default	120 mins

6.5.2.1.2 Transferring Option Board Codeplug File OTA

The transfer of an Option Board codeplug is quite different than transferring frequency files or Option Board firmware. This is because a codeplug transfer is a "Targeted" transfer to a specific, individual subscriber unit. The other transfers are called "Beaconed" transfers because the availability of these file types is beaconed on the control channel and all subscribers that determine that they need the file will join the transfer.

Prerequisites: Prior to initiating the Option Board codeplug file transfer, it is a very good idea to communicate with the radio user and to confirm that this is a good time to begin the codeplug file transfer. This is because the codeplug transfer will cause an interruption to service, and communicating this fact to the radio user increases the chances for a successful transfer.

When and where to use: The "*.efc" file that is transferred OTA is created specifically for the target subscriber unit using MOTOTRBO Connect Plus Option Board CPS. The standard codeplug format (*.cno) may not be transferred OTA. Therefore, it is necessary to create the *.efc file prior to attempting an OTA transfer of the codeplug.

Procedure:

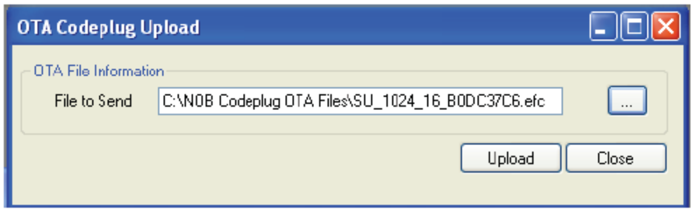
1 Locate the subscriber. The XRC will only accept the Option Board codeplug upload when the target subscriber unit is currently registered to its site. For multisite systems, it is necessary to locate the currently registered site of the subscriber unit using the **Find User** function from the Site Control menu. For a single site system, verify that the target subscriber unit is currently registered to the site prior to uploading the codeplug file. This can be verified through **Find User** or by viewing the list of registered users provided when selecting **Site Control** → **Status**.

2 After determining the subscriber's currently registered site, connect to the site where the unit is registered (if not already connected to that site).

3 Select **Site Control** in the Menu Bar.

4 Select **Upload** → **OTA Codeplug File**.

The OTA Codeplug Upload window appears.



File to Send C:\NOB Codeplug OTA Files\SU_1024_16_B0DC37C6.efc

5 Click the ... button to browse for and select the *.efc file. The file name must match the target SU. For example, a file name beginning with "SU_1024…" can be used for Radio ID 1024 only.

6 Click **Upload**. A series of checks are carried out. If a check fails, a notification screen is provided with the failure reason. If all checks are successful, an important message is displayed. The message must be acknowledged prior to continuing with the upload.

7 Read the important message, and click **Yes** to acknowledge the message.

8 Use the **Real Time Display** (RTD) to monitor the progress of the OTA Option Board codeplug file transfer. When the session is over, the RTD History and the Event Log will provide information on whether the codeplug transfer was successful. The XRC will not automatically re-attempt an unsuccessful OTA codeplug file transfer. You may re-upload the file to initiate another attempt.

For more important information on Option Board OTA Codeplug File Transfer, see the *MOTOTRBO Connect Plus System Planner*.

6.5.3 Uploading a Properties Change File

When and where to use: Uploading a Properties Change File is an advanced operation that should only be done at the direction of an authorized individual. Uploading this file will cause the device to reboot and to change one or more of its non-configurable properties or settings. Some configurable settings may also be affected.

NOTICE: The Properties Change File is created for a specific device. Uploading the file to any device other than the device it was created for will cause an error message to be displayed.

Procedure:

1. Obtain the Properties Change File from an authorized person and to place it in a known and accessible directory.
2. After connecting to the desired device, click on **Site Control** in the Menu Bar, and then select **Properties Change File** in the Upload submenu.

   The Properties Change File upload window is displayed.
3. Click the browse (**…**) icon to locate the `*.npf` file. After selecting the file, click **Open**.
4. Click **Upload**. A warning message is displayed. Read this important message carefully, as this will be the only opportunity to cancel the file upload.
5. Perform one of the following actions:
   - Click **Yes** to acknowledge the warning and proceed with the upload.
   - Click **No** or Cancel to abort the operation.

Upon receiving the uploaded file, the device performs some checks. If any check fails, the device does not update its properties or settings, but displays an error message. If all checks are OK, the device updates one or more of its non-configurable properties or settings and reboots.

6.5.4 Uploading/Upgrading Device Firmware

This section describes the procedure for Uploading, Removing, and/or Upgrading the firmware file (file extension `*.fir`).

When and where to use: For the 9100 model only, the same procedure is used for the Operating System upgrade file (file extension `*.osu`). Operating system upload and upgrade takes longer than the firmware upload and upgrade.

Procedure:

1. Obtain the new firmware file and place it in a known location on the PC.
2. Upload the firmware file to the device.See Uploading the Firmware File on page 151.
3. Run the command to upgrade to the uploaded firmware file. See Upgrading the Firmware on page 152.

   The upgrade command causes the device to reboot, and normal operation is disrupted. Although step 1 and step 2 can be done at any time, step 3 should be done at a time of low site usage.

6.5.4.1 Uploading the Firmware File

Prerequisites: Obtain the new firmware file and place it in a known file directory.

- Firmware files extension is `.fir`.
- Operating System upgrade file extension is `.osu`.

Procedure:

1. From the Menu Bar, select **Site Control** → **Firmware**.

   The **Firmware Manager** screen appears.

2. Click **Upload Firmware**.

   The **Open File** screen appears.

3. Browse to the directory containing the firmware file.
4. Select the file and click **Open**.

   A progress bar appears at the bottom of the screen showing the status of the upload, including an estimation of time remaining.

6.5.4.2

Removing a Firmware File

For efficient use of disk space, remove firmware files that are no longer needed.

Procedure:

1. From the Menu Bar, select **Device Control** → **Firmware**.

   The **Firmware Manager** displays.

2. Select the firmware file to be removed.
3. Click **Remove Firmware**.
4. Click **Yes** to confirm removal.

6.5.4.3

Upgrading the Firmware

When and where to use:

NOTICE: Upgrading to new Firmware causes the device to reset. This disrupts device communications for a short time.

Procedure:

1. From the Menu Bar, select **Site Control** → **Firmware**.

   The **Firmware Manager** window appears.

2. Select the firmware file to be sent to the device and click **Upgrade**.

   A dialog box appears, asking to confirm the upgrade.

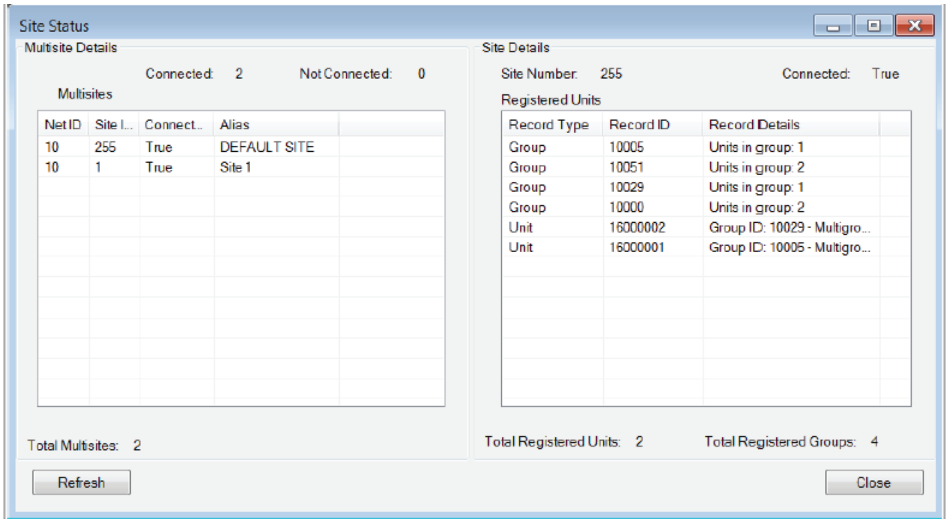
3. Click **Yes** to upgrade or **No** or **Cancel** to stop the upgrade.

6.5.5

Site Status Window

The **Site Status** window is divided into two parts.

Figure 57: Site Status Window



Multisite Details

Connected: 2 Not Connected: 0

Multisites

Net ID	Site I...	Connect...	Alias
10	255	True	DEFAULT SITE
10	1	True	Site 1

Total Multisites: 2

Site Details

Site Number: 255 Connected: True

Registered Units

Record Type	Record ID	Record Details
Group	10005	Units in group: 1
Group	10051	Units in group: 2
Group	10029	Units in group: 1
Group	10000	Units in group: 2
Unit	16000002	Group ID: 10029 - Multigro...
Unit	16000001	Group ID: 10005 - Multigro...

Total Registered Units: 2 Total Registered Groups: 4

Multisite Details Panel

The left side shows a list of network sites and the current status of the TCP connection to each site on the list. True indicates that there is currently a TCP/IP connection to the listed site. False indicates that there is not currently a TCP/IP connection to the listed site. If a row has a yellow background, this indicates that the IP address provided by the listed site is different than the site's IP address in the Multisite Configuration for this site (**Settings** → **Multisite**). This discrepancy may prevent voice calls from being connected and affect other communications between the two sites. It should be investigated further.

Site Details Panel

The right side shows a list of Units and Groups that are currently registered to the site that is selected on the left side of the window. If `[P]` appears next to a Group Record Type, this indicates the Group is on the Permanently Registered Groups list of the site.

IMPORTANT: The list of registered Units and Groups can change rapidly. Use the **Refresh** button to update the display. The display is not automatically updated when a Unit or Group registers or deregisters from a site.

6.5.5.1 Launching the Site Status Screen

Procedure:

From the Menu Bar, select **Device Control** → **Site Status**.

The **Site Status** screen appears.

6.5.5.2 Determining Connected Sites and Registered Units

Procedure:

1. From the Menu Bar, select **Site Control** → **Status**.

   The **Site Status** window appears.

2. Select a site in the Multisite Details panel.

   A list of the Users and Groups currently registered to that site appears in the Site Details panel.

3 The displayed information automatically refreshes upon selecting a different site in the Multisite Details panel. The displayed information does not automatically refresh just because a radio registers or deregisters with the site and/or network. Use the Refresh button to manually refresh the displayed information.

NOTICE: Clicking on the heading in panels sorts the information by that heading.

6.5.5.3

Traffic Slots Display

The bottom of the Site Status window includes a `Total Traffic Slots` display. The display shows how many repeater traffic slots have checked-in at currently connected sites. The count does not include Control Channel slots. This number is shown in the following format: `Current Total / Recommended Maximum`.

The maximum total number of slots in use should not exceed 770. Thus, if 400 slots are in use, the display shows: `Total Traffic Slots 400 / 770`

A warning icon (red exclamation point) appears if the current total exceeds 770. If you hover the mouse pointer over this exclamation point, a warning message appears telling you by how many slots you have exceeded the recommended maximum. Exceeding the maximum can result in undesirable system behavior.

6.5.6

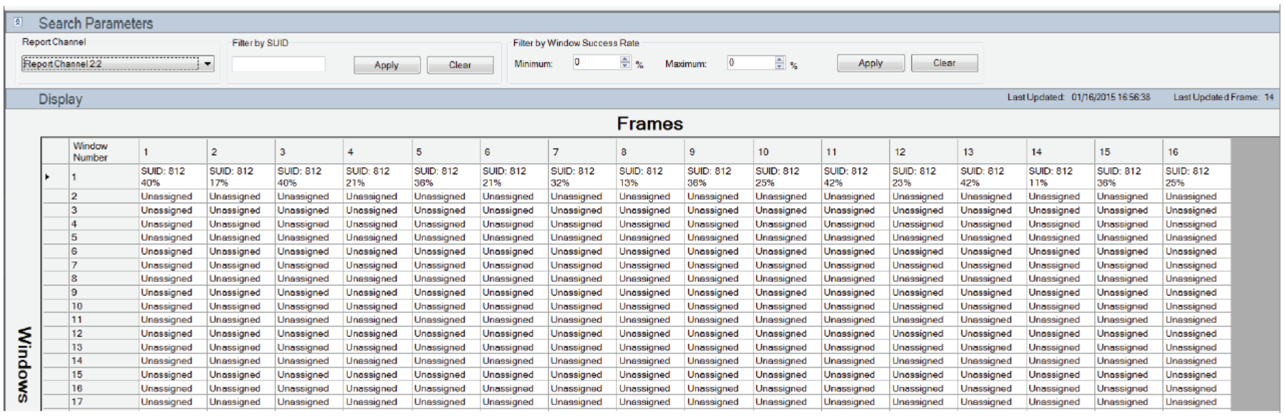
Fast GPS Tracking Window

The Fast GPS (Fast GPS) Report Channel Tracking Window provides data that can be used to help evaluate the performance of the selected Fast GPS Report Channel.

The Fast GPS Report Channel Tracking Window displays data about one Fast GPS Report Channel timeslot. When a site has multiple Fast GPS Report Channels, the Network Manager user can select which Report Channel data to display in the Fast GPS Tracking Window. Selecting a different Fast GPS Report Channel causes the Network Manager to replace the data from the previously selected Fast GPS Report Channel with the most-recently selected Fast GPS Report Channel.

The Fast GPS Tracking Window is divided into two major sections; the Search Parameters section and the Grid Display Section. See Search Parameters Section on page 155 and Grid Display Section on page 156.

Figure 58: Fast GPS Tracking Window



Report Channel: Report Channel 2:2

Minimum: 0 % Maximum: 0 %

Last Updated: 01/16/2015 16:56:38 Last Updated Frame: 14

Window Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	SUID: 812 40%	SUID: 812 17%	SUID: 812 40%	SUID: 812 21%	SUID: 812 36%	SUID: 812 21%	SUID: 812 32%	SUID: 812 13%	SUID: 812 36%	SUID: 812 25%	SUID: 812 42%	SUID: 812 23%	SUID: 812 42%	SUID: 812 11%	SUID: 812 36%	SUID: 812 25%
2	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned
3	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned
4	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned
5	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned
6	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned
7	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned
8	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned
9	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned
10	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned
11	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned
12	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned
13	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned
14	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned
15	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned
16	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned
17	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned

6.5.6.1

Launching the Fast GPS Tracking Window

Procedure:

1 From the Menu Bar, select **Site Control** → **Fast GPS Tracking Window**.

The Network Manager displays the **Fast GPS Tracking** window.

2 Click on **Report Channel** in the upper left-hand corner of the Fast GPS Tracking Window.

3 Select the Report Channel to be viewed from the drop-down list of currently active Fast GPS Report Channels.

6.5.6.2

Search Parameters Section

The **Search Parameters** section of the screen is located immediately above the **Grid Display** section. It contains the following fields and buttons:

Report Channel

Contains a drop-down list of Fast GPS Report Channels currently active on the site (by repeater and slot). If the Network Manager user selects a different Fast GPS Report Channel, the current data is replaced by data from the most-recently Fast GPS Report Channel.

Filter by SUID

Enter the SUID to be searched.

Apply

Initiates a search for cells containing the SUID that was entered into the **Filter by SUID** field. Any cells containing the SUID will be highlighted. If the entered SUID is found on a different Fast GPS Report Channel than the currently selected Fast GPS Report Channel, then Network Manager automatically updates the **Fast GPS Report Channel Tracking Window** with data for the Report Channel of the SU.

Clear

Clears the results of the previous SUID search.

Filter by Window Success Rate

For each assigned cell for which there is data, the Network Manager displays the percentage of reports received for the cell as compared to the reports requested for that SUID/Window/Frame combination. This percentage is referred to as the “success rate” of the cell. The calculated percentage is the percentage for this specific cell since it was assigned to this specific SU. The percentage is reset after each controller reboot, when the corresponding Fast GPS Report Channel is reallocated, or when a different SUID is assigned to the window.

The Network Manager user can search all cells on the display for a range of success rates (by expressing a “minimum” and “maximum” percentage), or for a specific success rate (by setting the “minimum” and “maximum” values to the same percentage).

Minimum

This is where the Minimum success percentage to be searched is entered by typing a numeric value between 0 and 100 percent, or by using the up/down arrows to select the desired percentage. The Minimum must be less than (or equal to) the Maximum.

Maximum

This is where the Maximum success percentage to be searched is entered by typing a numeric value between 0 and 100 percent, or by using the up/down arrows to select the desired percentage. The Maximum must be greater than (or equal to) the Minimum.

Apply

Initiates a search for cells within the specific range of success percentages. Any cells within the specified range will be highlighted.

Clear
Clears the results of the previous Success Rate search.

6.5.6.3
Grid Display Section

The **Fast GPS Tracking Window** Display area shows a grid that represents the Fast GPS superframe. The main components of the **Grid Display** are as follows:

Frames
The columns in the grid represent the Frames (1-16) in a Fast GPS Superframe.

Windows
The rows in the grid represent the Windows in a Fast GPS Superframe. The number of windows per frame varies according the Report Size configured in the Network Manager.

Individual Cells with the Grid
The intersection of the columns (Frames) and the rows (Windows) represent the individual cells within the superframe.

Horizontal Scroll Bar
When the Grid Display area contains more Frames than can be displayed in a single view, the Network Manager provides a horizontal scroll bar on the right-hand side of the screen.

Vertical Scroll Bar
When the Grid Display area contains more windows than can be displayed in a single view, the Network Manager provides a vertical scroll bar at the bottom of the screen

6.5.6.4
Fast GPS Tracking Display Data Interpretation

The Network Manager **Fast GPS Tracking** Display shows one superframe of Fast GPS data for the selected Report Channel. The Fast GPS radio trunks to its Fast GPS Report Channel and transmits a location report whenever it sees a window and frame to which it is assigned announced on the Control Channel time slot. When the controller announces the superframe, it starts by sending an announcement for Frame 1 and Window 1. The controller announces all of the Windows in Frame 1 before it starts announcing the Windows in Frame 2. This process continues until the controller has announced all windows (that is, all cells) in all 16 frames. Then it begins a new Superframe by announcing Frame 1 and Window 1 again.

The Network Manager does not update the **Fast GPS Tracking** Window after each individual window announcement. The Network Manager updates the displayed information one column of data (that is, one frame of data) at a time. Statistical data is reported by the controller 30 seconds after the frame ends, and each update contains 30-seconds worth of new data about a specific frame. The Network Manager provides an information bar above the grid display that contains a date and time stamp for when the grid was last updated, and it contains the Frame Number for the last updated Frame. If the last updated Frame was 5, for example, then the columns for Frames 1-5 contain information that has been updated during the current superframe. The columns for Frames 6-16 contain information that was last updated during the previous superframe. Whenever the Network Manager receives updated information for a frame, it overwrites any information that was previously displayed for the same frame number.

6.5.6.5
Data Displayed Within a Cell

Each cell within the superframe represents a time allotment where one radio can transmit one periodic location report on the selected Report Channel. The list below describes the information that can be displayed in a cell:

SUID

For each cell in the superframe, the Network Manager displays the SUID of the radio currently assigned to the cell. If there is no radio currently assigned to a cell, the Network Manager displays `Unassigned`.

Percentage (Success Rate)

For each assigned cell for which data has been received, the Network Manager displays the percentage of reports received for the cell as compared to the reports requested for that SUID/Window/Frame combination. The calculated percentage is the percentage for this specific cell since it was assigned to this specific SU. The percentage is reset after each controller reboot, when the corresponding Fast GPS Report Channel is reallocated, or when a different SUID is assigned to the window. When interpreting the displayed percentage, it is important to understand the following:

The displayed percentage refers to a single cell (that is, a specific SUID/Window/Frame combination). If a radio is assigned to more than cell within the superframe (which is common), it is not possible to determine the overall “reports received percentage” of the radio by reading the percentage of a single cell. To calculate the overall “reports received percentage” by the radio, it will be necessary to consider all of the cells assigned the same radio within the superframe.

When the system calculates the “received reports percentage”, a “received” report is any LRRP response received from the radio, even if the response doesn’t contain current location data (due to lack of a satellite fix or other reasons).

Exclamation Point Icon and Informational Messages

When a Fast GPS Report Channel Tracking Window contains additional information about a specific cell, the cell is highlighted and an exclamation point icon appears within the cell. Holding the mouse pointer over the exclamation point icon causes the Network Manager to display a message pertaining to this specific cell. See the *MOTOTRBO Connect Plus System Planner* for a discussion of these messages.

Occasional missed reports are a normal part of Fast GPS operation. If the controller does not know why it did not receive a report in a specific cell, the exclamation point icon is not displayed, and the Network Manager does not display any message containing additional information.

6.5.7 User Roles

6.5.7.1 User Roles Access

Each user roles has different sets of access. The following sections describe the access each user role has.

6.5.7.1.1 Administrator

Administrators have access to all features. Features exclusive to Administrators are:

- **Firmware Files:**
  - Uploading firmware files
  - Removing existing firmware files
  - Upgrading the XRC with a firmware file
- **Other File Uploads:**
  - Uploading Option Board Firmware files for over-the-air transfer
  - Uploading Option Board Codeplug files for over-the-air transfer
  - Uploading Network Frequency files for over-the-air transfer

  - Uploading XRC Properties Change Files
- **User Roles:**
  - Adding new users
  - Removing existing users
  - Changing passwords
- **Reset Site Configuration:**
  - Resetting Site Configuration to factory defaults
- **XRC Features:**
  - Enabling XRC Features

6.5.7.1.2 Manager

The following are features available to Managers.

- **User Registration:**
  - Viewing existing users/groups
  - Saving new/existing users/groups
  - Removing existing users/groups
  - Enabling/Disabling users
  - Copying the User Registry to other sites (with the User Health Tool)
- **Site Configuration:**
  - Saving configuration
- **Multisite Configuration:**
  - Saving new/existing sites
  - Removing sites
- **Network Settings:**
  - Viewing network settings
  - Saving network settings
- Rebooting the device
- **Date / Time Configuration:**
  - View date & time
  - Set date & time
- **Event Log Viewer:**
  - Clear event log
- **Alert Management:**
  - View, Refresh and Clear Active Alerts/Alarms
- **Alert Notifications:**
  - Save Alert Notifications
- **SMTP Setup:**
  - View SMTP Setup
  - Save SMTP Setup

- **Backup & Restore Utility:**
  - Save configuration to a file
  - Restore configuration from a saved file
- Switch to Primary/Secondary Controller

6.5.7.1.3 Monitor

Monitors only have access to view most features. They should not be allowed to make any modifications.

- **Site Configuration:**
  - View site configuration
- **Site Status:**
  - View site status
- **Real Time Display:**
  - View real time display
- **MultiSites:**
  - View MultiSites
- **Event Log Viewer:**
  - View Event Logs
- **Find Users:**
  - Locate a registered user
- **XRC Features:**
  - View XRC Features
- **Alert Management:**
  - View Active Alerts/Alarms
- **Alert Notifications:**
  - View Alert Notifications
- **Fast GPS Tracking Window:**
  - View Fast GPS Tracking Window

6.5.7.1.4 Accountant

Accountants only have access to download or clear Air Time Logs and Fast GPS Historical Logs.

6.5.7.1.5 User Setup

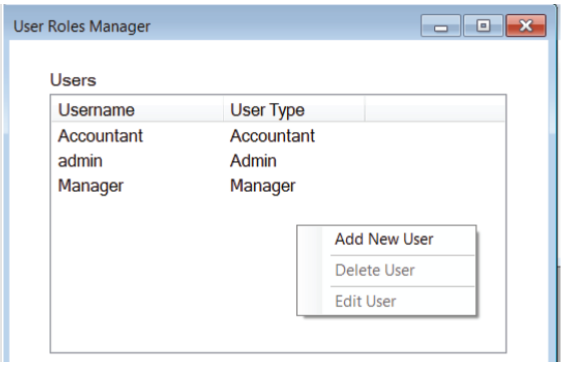
This section explains the steps to add and delete user roles as well as to change the password of users.

6.5.7.1.5.1 Adding a New User

Procedure:

1 From the Menu Bar, select **Site Control** → **User Roles**.

The **User Roles Manager** window appears.



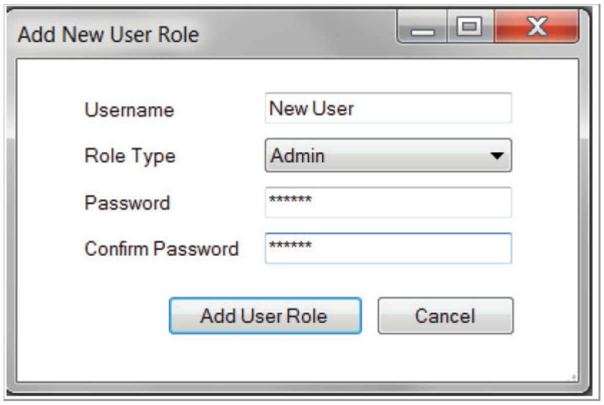
User Roles Manager

Users

Username	User Type
Accountant	Accountant
admin	Admin
Manager	Manager

2 Right-click anywhere within the window and select **Add New User** from the submenu.

The **Add New User Role** window appears.



Add New User Role

Username	New User
Role Type	Admin
Password	******
Confirm Password	******

3 Perform the following actions:

a Enter the User Name.

b Select **Role Type** from the drop down box.

c Enter the user password.

d Confirm the password.

4 Click **Add User Role**.

6.5.7.1.5.2 Deleting a User

Procedure:

1 From the Menu Bar, select **Site Control** → **User Roles**.

The **User Roles Manager** screen appears.

2 Right-click the **User Name** to be deleted.

3 Select **Delete User** from the sub-menu.

A dialog box asking to confirm the deletion appears.

4 Click **Yes** to delete a user.

6.5.7.1.5.3 Changing a Password

Procedure:

1 From the Menu Bar, select **Site Control** → **User Roles**.

2 Right-click the username to be changed and select **Edit User** from the submenu.

3 If the **Old Password** field appears, then enter the old password.

4 Enter the new password and confirm.

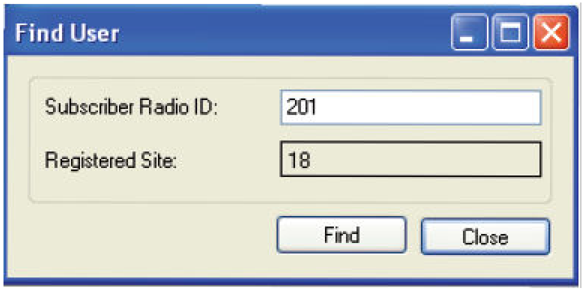
5 Click **Save Changes**.

6.5.8 Finding a User

Procedure:

1 From the Menu Bar, select **Site Control** → **Find User**.

The **Find User** window appears.



Subscriber Radio ID: 201

Registered Site: 18

2 Enter the **Subscriber Radio ID** in the field and click **Find**.

The registered site information is based on the most recent registration (or deregistration) of the subscriber with the Connect Plus network. The XRC does not perform a radio check to confirm to the presence of the subscriber prior to returning this information. It is therefore possible that the subscriber may have faded from network coverage since its last registration.

- If the unit is registered, the site number appears in the **Registered Site** field.
- If the unit is not registered, the response `Radio ID Not Registered` appears.
- If the unit does not exist in the XRC user database, the response `Radio ID Not Found` appears.

6.5.9 Switching To...

When and where to use:
In a redundant device configuration, the **Switch to** command is used to manually switch site control from one device to the other. The exact wording of the menu prompt depends which device you are connected to:

- When connected to the Primary device, and the Primary device currently has control, the menu item says, **Switch to Secondary Controller**.
- When connected to the Secondary device, and the Secondary device currently has control, the menu item says, **Switch to Primary Controller**.
- When connected to a Stand-alone device, this menu item is grayed out.

Procedure:

1. Select **Site Control** in the main menu.
2. Select **Switch to** (Primary or Secondary Device).
3. A warning message appears. Acknowledge the message to proceed with the switch. This will cause the connected device to reboot, and you will be disconnected from the device.

IMPORTANT: Switching device control causes a temporary interruption to service. Subscriber radios that were registered to the site will enter search mode. If there is overlapping coverage with another network site, the switch over may cause some radios to change sites. See the *MOTOTRBO Connect Plus System Planner* for important information.

6.5.10 User Health Tool

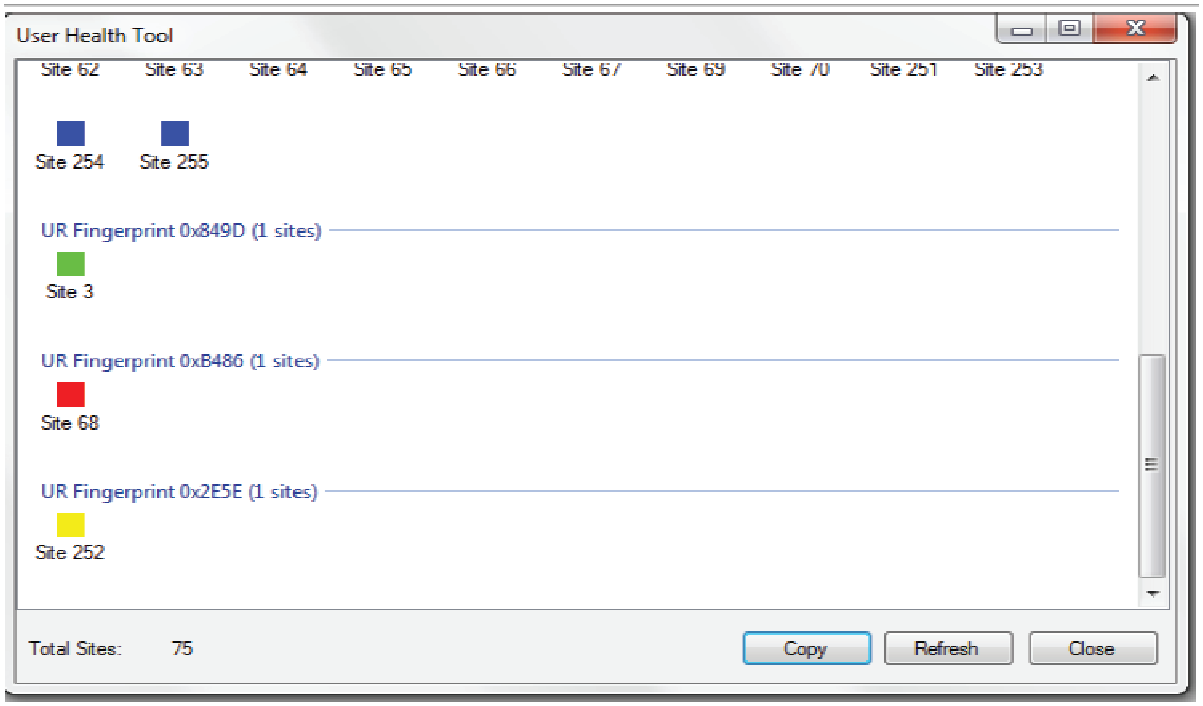
In multisite networks, it is imperative that all sites maintain an identical copy of the User Database (also called the "User Registry"). This is the database of subscriber radios, talkgroups, multigroups, pool IDs, private talkpath IDs, etc. In normal operation the sites automatically share updates to the database and keep one another synchronized.

If site links are disrupted or there are other problems that prevent the normal synchronization of the user databases between sites, there is a possibility that the user databases may become out of "sync" for some sites. Symptoms of an out of sync condition would include subscribers being denied registration at one site but not others, multisite talkgroup calls not being propagated to sites that seem to have registered members, etc.

The **User Health Tool** is used to determine the state of database synchronization between sites as well as remedy any out of sync conditions that persist over an extended period of time. The User Health Tool should be run any time there has been a failure in network connectivity or in site infrastructure that could have disrupted the normal synchronization process and when the User Registries of the network sites do not automatically synchronize after network connectivity is re-established. If the XRC and XRT firmware is from Connect Plus System Release 1.6 or later, this automatic synchronization will typically not require any user intervention, and it will not be necessary to utilize the User Health Tool. The amount of time required for the automatic synchronization of the User Registries at all network sites depends on the number of sites in the network, and the number of adjustments that the sites must make to their User Registries.

When the User Health Tool is selected from the **Site Status** dropdown menu, the site controller polls all of the other sites in its Multisite table to determine their user database status. When complete, a window similar to the following figure appears.

Figure 59: User Health Tool Screen



Total Sites: 75

In the window, sites are grouped according to their synchronization status. Sites that share identical databases are grouped together and assigned the same color. The colors are assigned arbitrarily and have no particular meaning. Also, each site grouping that has an identical copy of the user database shares the same "UR Fingerprint"; which is expressed as a hexadecimal number. Normally, all sites will be grouped together and assigned to a single color and share the same UR Fingerprint. This indicates no need for further action as all databases are in sync. If there are multiple groups of sites, this indicates that each discrete group has a different "version" of the user database. This would indicate that you must perform a database synchronization between the sites. In addition, any sites that are unable to be polled are grouped together as "Unreachable" sites since their database synchronization status cannot be determined. If any sites are currently involved in the User Health sync process, they are grouped under the heading, "Site Locked".

IMPORTANT: When a User Registry of a site is locked because it is the source or target site for User Health Sync (or because the site controller is automatically synchronizing its User Registry with another site controller), the Network Manager does not allow the user database to be edited. If the user attempts to edit a record while the User Registry is locked, an error message will be displayed. If this occurs, wait for the sync process to complete and try again later.

6.5.10.1
Copying the User Registry

When and where to use: Do not close the **User Health Tool** window or disconnect the Network Manager during this process. If this should occur, the transfer in progress will complete, but other transfers on the list (ones that have not started yet), will be canceled.

Procedure:

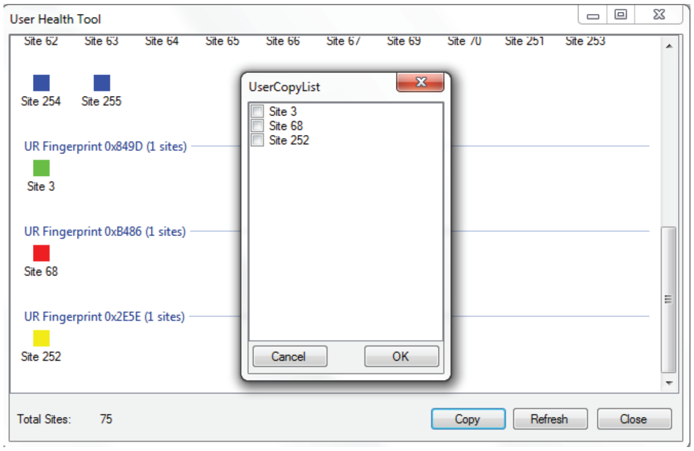
1 While connected to the site that has the "master" copy of the user database, select **Site Control → User Health Tool**.

While some actions cause the window to refresh automatically, some other actions do not (such as editing records at a different site or when a radio user issues an "enable" or "disable" command over-the-air). For this reason, the window provides a **Refresh** button to update the displayed groupings and site information.

The **User Health Tool** window opens, containing the information described above.

2 After determining that one or more sites need to be updated with the user database of the connected site, click **Copy**.

The **User Copy List** window opens. The window shows a list of reachable sites that have a different database "fingerprint" than the site to which you are connected.



Total Sites: 75

3 Place a check next to each site that you wish to update. Click **OK** to proceed.

A Warning message appears to advise you that updating a site's user registry causes the target site to be unusable for a period of time.

4 Click **Yes** to continue, or **No** or **Cancel** to abort the procedure.

5 During the sync process, a new panel opens on the right-hand side of the screen. The panel contains a list of each site selected for updating. The user database of each site on the list is updated, one site at a time. The transfer currently in progress shows the percentage complete.

Once the synchronization is complete for a target site, the right-hand panel shows "Transfer Complete" next to the site number. The display will update as the target site Reboots and is temporarily listed as "unreachable". When the target site has completed its reboot, the display updates again, and the target site will be grouped with the other sites that are in sync with the source site.cBoth sites will be locked to any database updates during the synchronization process.

6.5.10.2 Using the User Health Tool to Update the User Database of XRT Gateway Site(s)

XRT Gateway Sites are identified by their special site numbers (251-255).

If using the Network Manager User Health Tool to update the user database of any XRT Gateway site, do not include the XRT in a list of sites to be updated. Update the XRT sites one at a time, and allow the update to complete and the XRT to reboot and come back on-line prior to starting the next user database update.

Be advised that updating the user database of the XRT may change the UR Fingerprint of all other sites. This results from the Talk Path re-registrations that follow the XRT reboot, and is a normal part of XRT operation. In most cases the network will synchronize the Fingerprints automatically. Do not use the User Health tool to copy any user database while this automatic synchronization process is underway.

6.5.11 Reset Configuration

Reset Configuration provides a way to return certain settings to factory defaults. This should not be performed on a deployed XRC, as this would cause operational issues. After returning the settings to factory defaults, it will be necessary to re-configure the affected settings to the desired values.

6.5.11.1 Resetting Site Configuration Settings

When and where to use: This menu option is used to reset configurable settings to factory defaults. This operation should not be performed on a currently deployed XRC. Resetting the configurable settings to factory defaults can prevent radios from using the XRC and impact networking with other sites. This operation will also cause the XRC to reboot. After using this feature, it will be necessary to re-configure the settings to the desired values.

Procedure:

1. From the Menu Bar, select **Site Control** → **Reset Configuration**.
2. Select **Reset Site Configuration** from the sub-menu.

   The Network Manager displays a warning message.

   ⚠ **CAUTION:** Read this important message carefully as this will be the only opportunity to cancel the operation. Do not perform this operation on a currently deployed (operational) site!

3. Click **Yes** to acknowledge the warning and proceed with the operation, or click **No** or **Cancel** to abort the operation.
4. After the XRC reboots, you will need to reconnect and manually configure the configurable settings to the desired values.

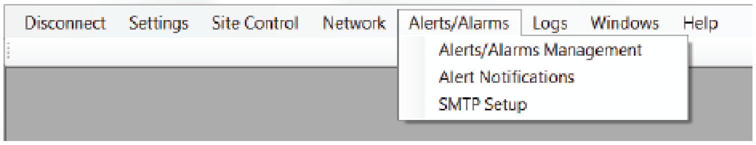
Postrequisites: It will be necessary to re-configure the Site Configuration settings to the desired values.

6.6 Alerts and Alarms Management

6.6.1 Overview

Alerts are generated by the device in response to various conditions. Alerts can be managed at the Alert Management window. The following figure shows the drop down menu where the **Alert Management** window can be found.

Figure 60: Alerts/Alarms Management Option in the Drop Down Menu



The device may be configured to send e-mail Alert Notifications to interested parties when an Alert is raised.

If the site has both a Primary and Secondary device in a redundant configuration, Alerts/Alarms can be viewed and managed on the active device only (that is, the device that is currently in charge of the site.) When a device changes to the inactive state, it clears any Alerts that may have been active.

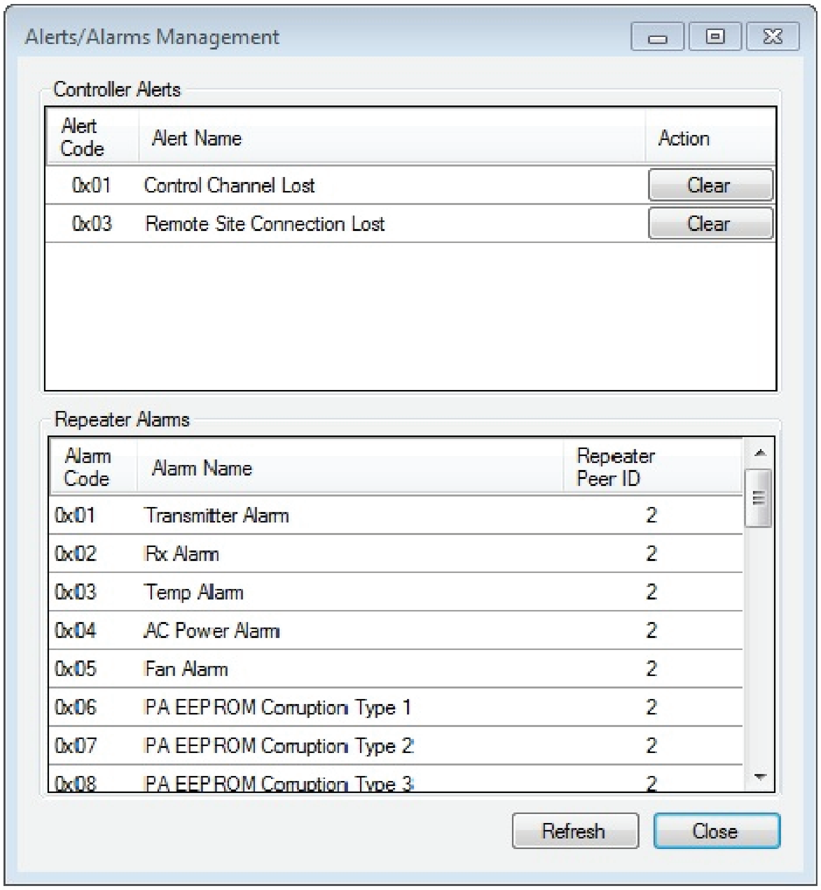
6.6.2 Launching the Alerts/Alarms Management Window

Procedure:

1 Click on **Alerts/Alarms** in the menu bar.

2 Select **Alerts/Alarms Management** from the dropdown menu.

The Alerts/Alarms Management window appears. The top portion of the window shows any active Controller Alerts. The bottom portion of the window shows any active Repeater Alarms.



Controller Alerts

Alert Code	Alert Name	Action
0x01	Control Channel Lost	Clear
0x03	Remote Site Connection Lost	Clear

Repeater Alarms

Alarm Code	Alarm Name	Repeater Peer ID
0x01	Transmitter Alarm	2
0x02	Rx Alarm	2
0x03	Temp Alarm	2
0x04	AC Power Alarm	2
0x05	Fan Alarm	2
0x06	PA EEPROM Corruption Type 1	2
0x07	PA EEPROM Corruption Type 2	2
0x08	PA EEPROM Corruption Type 3	2

6.6.2.1 Controller Alerts

A Controller Alert is raised when an underlying fault condition occurs. There may be several different faults that can trigger the same category of Controller Alert. For example, any Repeater Alarm reported by the repeater to the XRC will raise the `Repeater Alarm Detected` Controller Alert. It is necessary to view the site's Event Log to see which specific repeater alarm may have raised the Controller Alert. Additionally, if multiple repeater alarms occur while the `Repeater Alarm Detected` Controller Alert is still active, there will be a separate Event Log entry for each Repeater Alarm, but the Controller Alert will be raised only once.

Once a Controller Alert is raised, it stays active until manually cleared by the Network Manager user. This operation has several implications for the Network Manager user:

1. The underlying fault that triggered the Controller Alert may or may not be still present. It is the technician's responsibility to investigate further.
2. Once the technician has confirmed that the underlying fault is no longer present, he/she must manually clear the Controller Alert.
3. If the underlying fault condition is still present when the technician clears the Controller Alert, raise the Controller Alert again. This bears further investigation.

Alert Message	Description
Control Channel Lost	This alert occurs if the site operates without a Control Channel for more than 1 minute.
Repeater Alarm Detected	This alert occurs if a repeater detects a fault in its operation.
Remote Site Connection Lost	Occurs if a remote site has lost connection for more than 1 minute.
Secondary Controller Active	This alert is shown by the Secondary Controller, after it takes over site control from the Primary Controller.
Primary Controller missing connected Secondary Controller	Indicates that the Primary Controller hasn't yet communicated with the Secondary Controller, or that communication has been established, but the process of synching with the Secondary Controller is not yet complete.
Emergency Configuration Error	A radio sent a request for Emergency Alert or Emergency Call and the XRC detected a configuration error. See the **Event Log** for the following details: **1** the Source Radio ID **2** the Destination Group ID **3** the error reason To correct the Emergency Configuration Error it may be necessary to edit one or more user records (using the Network Manager), and/or to edit the Option Board codeplug (using Connect Plus CPS). If the underlying problem is not corrected, the Emergency Configuration Error will be raised again the next time the radio attempts to send an Emergency Call or Emergency Alert.
System Health Alert	This alert is raised upon detection of certain conditions that may be detrimental to the hardware or software performance. When the alert is raised, an **Event Log** entry is also created. The entry contains a "System Health issue number" that can be provided to Motorola Solutions technical support personnel for further investigation.
Repeater Controller Mode Error	This alert is raised when a repeater checks-in with the XRC, and the repeater's firmware level supports the "System Controller Mode" configurable setting, but the setting is **not** currently enabled in the repeater's codeplug. When the alert is raised, an Event Log entry containing the Repeater ID (Radio ID) is generated. "System Controller Mode" must be enabled in the repeater's codeplug with MOTOTRBO CPS before the repeater can be used as a Connect Plus over-the-air resource.

NTP Server Conflict	This event is raised when a site that is configured as NTP Server detects that another site has also been configured as NTP Server. This is a configuration error since no more than one device should be configured as NTP server in the Connect Plus network. When the alert is raised, the device also creates an Event Log entry to capture the site number of the other device that is also configured as NTP Server. This should be investigated and resolved so that the network does not have more than one NTP server. **NOTICE:** It is allowable to configure both devices in a redundant pair as NTP server since only one of the two devices will be active at a time.

6.6.2.2 Repeater Alarms

Repeater Alarms indicate some type of fault in repeater operation. In most cases, the repeater reports the alarm to the XRC, which causes the controller to create an **Event Log** entry for the specific alarm and to raise the generic `Repeater Alarm Detected` Controller Alert (if not already active). Depending on severity, Repeater Alarms may or may not result in an interruption to service. In all cases, the underlying fault should be further investigated. Using the **Event Log** viewer is a good place to start. Reference the Alarm Code and the Alarm Name (if provided) when speaking with support personnel. Repeater Alarms differ from Controller Alerts in a couple of important ways:

1. If a Repeater Alarm is displayed, the underlying fault is likely still active. (It is possible that the fault has been addressed, but the repeater has not yet reported this to the XRC.)
2. The technician cannot clear the Repeater Alarm from this screen. The Repeater Alarm must be cleared in some other fashion. The XRC will clear the alarm if the repeater reports that the alarm is no longer active, or if the repeater completes a subsequent Link Establishment and the alarm is no longer active.

6.6.2.3 Refreshing the Alerts Window

Once the Alerts/Alarms Management window has been opened, the list of active alerts do not update automatically (if a new alert is raised on the connected device).

Procedure:

Click **Refresh** to request the device software and device to update the list.

6.6.3 Alert Notifications (Email)

The device is capable of sending Alert notifications via email. The first step is to setup the SMTP Server. The next step is to setup Notification Groups to receive Alert Notifications. This is accomplished with the Alert Notifications screen.

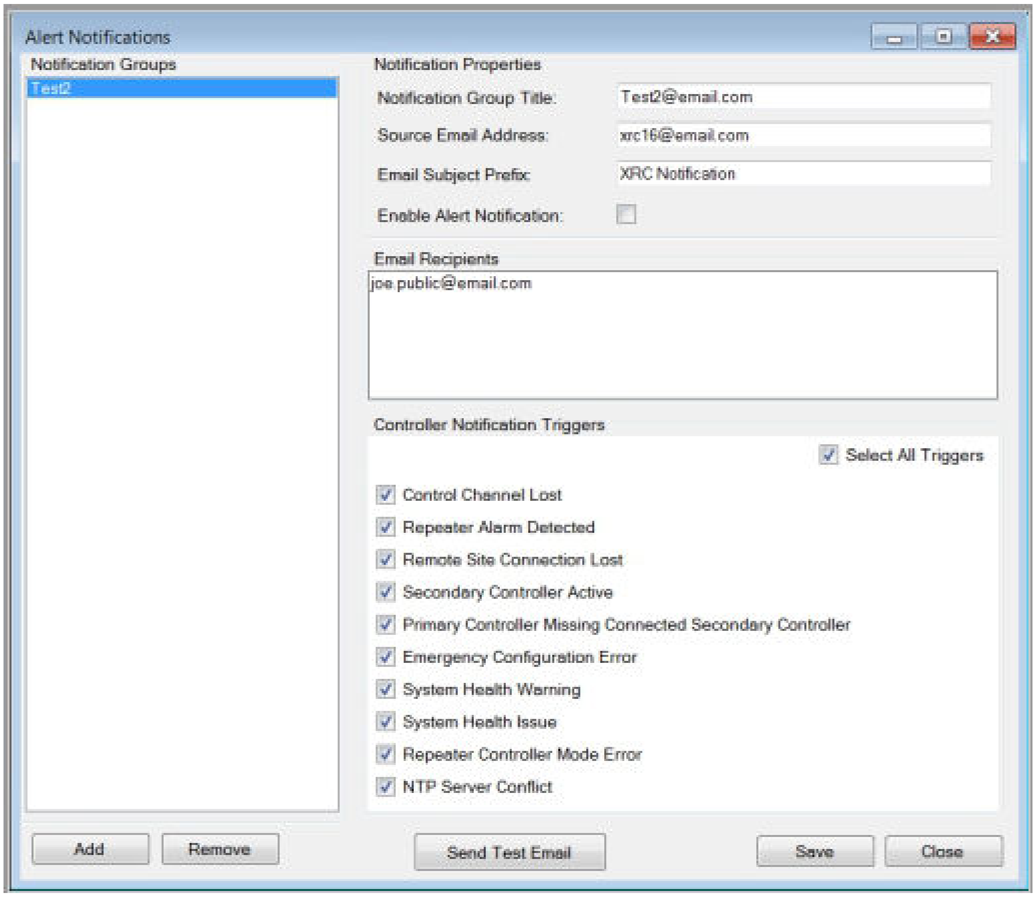
Notification Group

This is the name of the structure used to create and configure an Alert Notification. It is called a Notification Group, because the Alert Notification can be sent to multiple email addresses. Up to five Notification Groups can be created per site, and each Notification Group can be configured for up to 20 email recipients.

Alert Notification

An Alert Notification is an email that is sent automatically by the device when an Alert is raised. When creating/configuring a Notification Group, the software tool user configures which Alert(s) will trigger a notification email. If multiple Alerts are configured to trigger an email, there will be a separate email for each Alert that is raised. The email subject line tells which type of Alert has triggered the email and what site the alert occurred at. In addition, the subject line can be configured by the software tool user to include additional information (Email subject prefix). The email body is blank. The email does not contain specific information regarding which underlying fault raised the Alert. It is possible that multiple faults have occurred within the same Alert category. In this case, the Alert is only raised when the first fault occurs (assuming that the user has not yet cleared the Alert). The technician should use the software tool to connect to the indicated site and investigate further.

Figure 61: Alert Management Window



Notification Groups
Test2

Notification Properties
Notification Group Title: Test2@email.com
Source Email Address: xrc16@email.com
Email Subject Prefix: XRC Notification
Enable Alert Notification: □

Email Recipients
joe.public@email.com

Controller Notification Triggers
☑ Select All Triggers
☑ Control Channel Lost
☑ Repeater Alarm Detected
☑ Remote Site Connection Lost
☑ Secondary Controller Active
☑ Primary Controller Missing Connected Secondary Controller
☑ Emergency Configuration Error
☑ System Health Warning
☑ System Health Issue
☑ Repeater Controller Mode Error
☑ NTP Server Conflict

Existing Notification Groups are shown in the column on the left. Click an existing group to edit its properties.

6.6.3.1

Creating Alert Notification Groups

Procedure:

1. Click the **Add** button.
2. Enter a **Notification Group Title**.
3. Enter the **Source Email Address**. This is the "From" address that will be shown to recipients of the alert notifications.

Not all SMTP hosts allow a "From" address that is different than the user's email account on the host server.

4 Enter a **Subject Prefix**. This may be useful for recipients who sort their incoming messages based on the prefix. The Subject Prefix will precede the subject that is automatically generated by the device.

5 Check the box labeled **Enable Alert Notification** if you are ready for the device to start generating emails to this Alert Group after saving the information (assuming that a prerequisite Alert trigger occurs). Uncheck the box if you want the device to retain the information (after you finish configuring this screen and click **Save**), but you are not ready to start generating emails to the Alert Group.

6 In the field labeled **Email Recipients**, enter email addresses in the standard email address format. Separate the entries with either a semicolon or a comma. Placing a space prior to subsequent email addresses in the string helps makes them more readable, but is not required.

7 Select **Triggering Events**. Check the boxes for each Alert that you wish to trigger a group notification, or check the box labeled **Select All Triggers**.

8 If desired, click **Send Test Email** to generate a test email to the email addresses in this Notification Group. This action automatically opens the **Alert Notification Tester Window**. At the top of the window, under **Status**, look for the result of the test (either `Test Completed Successfully` or a failure notice). `Test Completed Successfully` means that the email was acknowledged by the SMTP Server. It does not necessarily mean that the email arrived at the Inbox of the intended recipient(s). Ask a recipient to check his/her Inbox to determine whether the email reached its final destination. The **Email Log** portion of the window displays some debug information which can assist an IP specialist, knowledgeable in SMTP, with debugging the test email process. When finished, close the **Alert Notification Tester** window to return to the **Alert Notifications** screen.

9 Click the **Save** button on the **Alert Notifications** screen when finished.

6.6.4 Setting Up SMTP for Email Notifications

An external SMTP host is necessary in order to send alert emails. The SMTP host must be reachable from the device that is being configured. Consult the IT manager (or knowledgeable individual) of your company to know what information should be entered when configuring this screen.

When and where to use:

NOTICE: While the device is able to automatically send emails, it is not capable of receiving emails. This includes emails that may be automatically generated by the SMTP Host (such as notifications of failed delivery).

Procedure:

1 Enter the SMTP Host Name (for example, smtp.domain.com) or IP address.

Entering a Host Name requires the device to be configured with a valid Nameserver (reachable by this device) under **Network** → **Settings**.

2 Enter the port number on which the host listens for incoming mail.

3 Check **Authentication Required** if the host requires the device to login with a Username and Password.

Checking this box activates the **Username** and **Password** fields.

4 If Authentication is required, enter the Username and Password the device should use when logging in with the SMTP Host.

5. If the SMTP Host requires Secure Sockets Layer (SSL), check the box labeled **SSL Connection**.
6. If the SMTP Host requires Transport Layer Security (TLS), check the box labeled **TLS Connection**.
7. Click **Save** when finished.
8. To test the SMTP Setup (assuming that the SMTP Host is currently reachable from the device and that all necessary accounts have been created), use the **Alert Notifications** screen to create a Notification Group and send a test email.

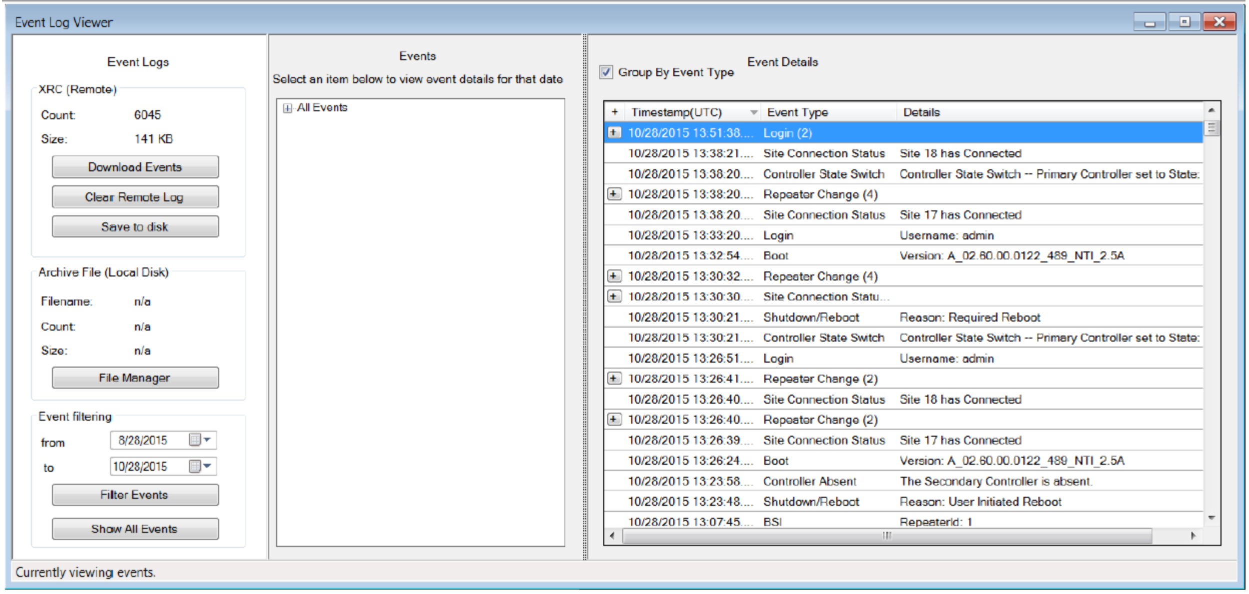
6.7 Logs

This section explains the viewing and management of various logs.

6.7.1 Event Log Viewer

The **Event Log Viewer** has three panels: **Event Logs**, **Events** and **Event Details**.

Figure 62: Event Log Viewer Window



XRC (Remote)

Count: 6045

Size: 141 KB

Archive File (Local Disk)

Filename: n/a

Count: n/a

Size: n/a

Event filtering

from 8/28/2015

to 10/28/2015

Select an item below to view event details for that date

☑ Group By Event Type

+	Timestamp(UTC)	Event Type	Details
⊞	10/28/2015 13:51:38....	Login (2)	
	10/28/2015 13:38:21....	Site Connection Status	Site 18 has Connected
	10/28/2015 13:38:20....	Controller State Switch	Controller State Switch -- Primary Controller set to State:
⊞	10/28/2015 13:38:20....	Repeater Change (4)	
	10/28/2015 13:38:20....	Site Connection Status	Site 17 has Connected
	10/28/2015 13:33:20....	Login	Username: admin
	10/28/2015 13:32:54....	Boot	Version: A_02.60.00.0122_489_NTI_2.5A
⊞	10/28/2015 13:30:32....	Repeater Change (4)	
⊞	10/28/2015 13:30:30....	Site Connection Statu...	
	10/28/2015 13:30:21....	Shutdown/Reboot	Reason: Required Reboot
	10/28/2015 13:30:21....	Controller State Switch	Controller State Switch -- Primary Controller set to State:
	10/28/2015 13:26:51....	Login	Username: admin
⊞	10/28/2015 13:26:41....	Repeater Change (2)	
	10/28/2015 13:26:40....	Site Connection Status	Site 18 has Connected
⊞	10/28/2015 13:26:40....	Repeater Change (2)	
	10/28/2015 13:26:39....	Site Connection Status	Site 17 has Connected
	10/28/2015 13:26:24....	Boot	Version: A_02.60.00.0122_489_NTI_2.5A
	10/28/2015 13:23:58....	Controller Absent	The Secondary Controller is absent.
	10/28/2015 13:23:48....	Shutdown/Reboot	Reason: User Initiated Reboot
	10/28/2015 13:07:45....	BSI	RepeaterId: 1

Currently viewing events.

Event Logs

On the Left hand side of the Event Log Viewer is the Event Logs panel. Within this panel, event logs are loaded from the device or local PC. Event filtering is also available to aid searching large event logs.

XRC (Remote)

Count: Displays the number of events currently on the device.

Size: Displays the Event Log file size on the device in Bytes.

NOTICE: When the Event Log archive exceeds the maximum allowed size (which can vary by device type and release) the oldest entries are automatically purged. For this reason, it is recommended to: (a) download events on a regular schedule and (b) clear the Log after downloading events.

Events and Events Details

The **Events** panel is first populated with information in a collapsed form. Click the **+** next to **All Events** to see a list of one or more years in which the downloaded events were recorded. The next level will be the month(s) and then the day(s) of the month. The results are displayed in the **Event Details** panel as the different headings are selected.
The Event Details panel contains a checkbox called **Group By Event Type**. When the box is checked, consecutively listed events of the same Event Type are collapsed into a single entry. The number of events contained within the collapsed entry is shown in parenthesis next to the **Event Type**. Click **+** to the left of an entry to show all of the consecutively listed events of the same Event Type. To collapse the events into a single entry again, click the **-** to the left of an entry.

6.7.1.1 Event Logs

The **Event Logs** panel is located on the left side of the **Event Log Viewer** window. Event logs are loaded from the device or local PC. Event filtering is available to improve searching for large event logs.

6.7.1.1.1 XRC (Remote)

Count displays the number of events currently on the XRC and Size displays the size of those events (in Bytes) on the XRC.

NOTICE: When the Event Log archive exceeds the maximum allowed size (which can vary by device type and release) the oldest entries are automatically purged. For this reason, it is recommended to: (a) download events on a regular schedule and (b) clear the Log after downloading events.

6.7.1.1.1.1 Events and Events Details

The Events panel is first populated with information in a collapsed form. Click the **+** next to **All Events** to see a list of one or more years in which the downloaded events were recorded. The next level will be the month(s) and then the day(s) of the month. The results are displayed in the **Event Details** panel as the different headings are selected.

The Event Details panel contains a checkbox called **Group By Event Type**. When the box is checked, consecutively listed events of the same Event Type are collapsed into a single entry. The number of events contained within the collapsed entry is shown in parenthesis next to the **Event Type**. Click the **+** to the left of an entry to show all of the consecutively listed events of the same Event Type. To once again collapse the events into a single entry, click the **-** to the left of an entry.

6.7.1.1.1.2 Downloading Events

Procedure:

1. From the Menu Bar, select **Logs** → **Event Log Viewer**.

   The **Event Log Viewer** window appears.

2. In the **Event Log** panel, click **Download Events**.

   Event information is displayed on both the **Event** and **Event Detail** panels.

6.7.1.1.1.3 *Clearing Remote Logs*

Procedure:

1 From the Menu Bar, select **Logs** → **Event Log Viewer**.

The **Event Log Viewer** window appears.

2 In the **Event Log** panel, click **Download Events**.

3 In the **Event Log** panel, click **Clear Remote Log**.

A dialog box asking to confirm the deletion appears.

4 Click **Yes** to clear all events.

Event information, if downloaded, is cleared on both the **Event** and **Event Detail** panels.

6.7.1.1.1.4 *Saving to Disk*

Procedure:

1 From the Menu Bar, select **Logs** → **Event Log Viewer**.

The **Event Log Viewer** window appears.

2 In the **Event Log** panel, click **Download Events**.

Event information is displayed on both the **Event** and **Event Detail** panels.

3 Click \ **Save to disk**.

The file is saved in the MOTOTRBO Connect Plus Network Manager folder in the following format: `EA`***`<mm-dd-yy>-<hh.mm.ss>`***, where ***`<mm-dd-yy>`*** is the date and ***`<hh.mm.ss>`*** is the time. The **Save to disk** button is grayed out until events are downloaded from the device.

6.7.1.2 Archive File (Local Disk)

This area allows access to saved event logs.

6.7.1.2.1 Loading an Archive File

Procedure:

1 From the Menu Bar, select **Logs** → **Event Log Viewer**.

The **Event Log Viewer** window appears.

2 In the **Event Log** panel, click **File Manager**.

The **Event Archive File Manager** window appears.

3 Click the file name of the event archive to be displayed.

4 Click **Load Selected**.

Event information is displayed on both the **Event** and **Event Detail** panels.

6.7.1.2.2 Deleting an Archived File

Procedure:

1 From the Menu Bar, select **Logs** → **Event Log Viewer**.

The **Event Log Viewer** window appears.

2 In the **Event Log** panel, click **File Manager**.

The **Event Archive File Manager** window appears.

3 Click the file name of the event archive to be deleted.

4 Click **Remove Selected**.

A message box asking to confirm the deletion appears.

5 Click **Yes** to delete the event archive.

6 To close the **Event Archive File Manager** dialog box, click the **X** in the upper right corner.

6.7.1.3 Filtering Events

Procedure:

1 From the Menu Bar, select **Logs** → **Event Log**.

The **Event Log Viewer** window appears.

2 In the **Event Log** panel, perform one of the following actions:

- Click **Download Events**.
- Click **File Manager** and load the saved archived file.

Event information is displayed on the **Event** and **Event Detail** panels.

3 Select a beginning date from the **From** field.

4 Perform one of the following actions:

- Select an ending date for the **To** field and click **Filter Events**.
- Click **Show All Events** to see all events.

The selected range of events are shown in the **Event Detail** panel.

6.7.2 Air Time Logging

This section describes the management of air time logs.

6.7.2.1 Saving As...

The **Save As** option opens a window that allows the Air Time Logging data to be saved to the PC in .ATR file format.

Procedure:

1 From the Menu Bar, select **Logs** → **Air Time Logs** → **Save As**.

2 Choose the file locations and click **Save**.

Once the file has been saved, Windows Explorer® automatically opens to the default file location.

6.7.2.2
Exporting To

The **Export To** option opens a window that allows the Air Time Logging data to be saved to the PC in comma delimited (.CSV) file format.

Procedure:

1 From the Menu Bar, select **Logs** → **Air Time Logs** → **Export To**.

2 Choose the file locations and click **Save**.

Once the file has been saved, Windows Explorer® automatically opens to the default file location.

6.7.2.3
Clearing Logs

The **Clear Logs** command informs the XRC to clear the Air Time Logging data.

When and where to use: The **Clear Logs** command informs the XRC to clear the Air Time Logging data. This is recommended after downloading air time data so that the next download includes only the air time accumulated since the **Clear Logs** command.

Procedure:

1 From the Menu Bar, select **Logs** → **Air Time Logger** → **Clear Logs** .

   A confirmation message appears.

2 Click **Yes** to clear logs or **No** or **Cancel** to stop clearing logs.

   The following message appears: `Air Time Logs cleared successfully!`

6.7.3
Fast GPS Historical Data Logs

6.7.3.1
Saving Fast GPS Historical Data

This opens a window that allows Fast GPS Historical Data to be saved to the PC in .BIN file format.

Procedure:

1 From the Menu Bar, select **Fast GPS Historical Data Logs** → **Save As…**.

2 Chose the file locations and click **Save**.

Once the file has been saved, Windows Explorer® will automatically open to the default file location.

6.7.3.2
Exporting Fast GPS Historical Data Logs

This opens a window that allows Fast GPS Historical Data to be saved to the PC in comma delimited (.CSV) file format.

Procedure:

1 From the Menu Bar, select **Fast GPS Historical Data Logs** → **Export to…**.

2 Chose the file locations and click **Save**.

Once the file has been saved, Windows Explorer® will automatically open to the default file location.

6.7.3.3 Clearing Fast GPS Historical Data Logs

This command tells the controller to clear Fast GPS Historical Data.

Procedure:

1 From the Menu Bar, select **Fast GPS Historical Data Logs** → **Clear Logs**.

   A confirmation message will appear.

2 Perform one of the following actions:

   - Answer **Yes** to clear logs.
   - Answer **No** or **Cancel** to stop clearing logs.

6.8 Date Time Configuration

The top (gray) portion of the screen shows the current date and time on the connected device. The device does not use local time. Instead, it uses Coordinated Universal Time (UTC), an international standard that correlates with time at the Royal Observatory in Greenwich, England. This is the time displayed on the top line in the gray box. On the second line in the gray box, the device software adjusts the hour to reflect the hour and time zone on the PC's clock at time of connection. The minutes and seconds are derived form the current time of the device

The bottom (white) part of the screen shows the current date and time for the PC running the device software. This portion of the screen allows the user to transfer the PC's date and time to the device. If this device is set as the NTP Server, updating the date and time on the device will also affect all sites that are programmed to look at this site as the NTP Server. Those sites will receive the updated date and time the next time they request a time update. Due to the normal operation of the NTP Protocol, it may require multiple updates to bring the Server and Client into synch if the two clocks are far apart to begin with. For this reason, it is advisable to set the time on the NTP Client during initial set-up as described in the next section. Although the NTP Client's time will be adjusted by the NTP Server, the time synchronization will occur more quickly if the time on the two clocks is within a few minutes of one another to begin with.

IMPORTANT: When transferring the PC's date and time to the device (by following the procedure described in the next section), the device software will correctly adjust the PC's date and time to UTC provided that:

- The date and time settings of the PC are accurate for the time zone that is configured for on the PC **Date and Time Properties** screen.
- The **Automatically adjust clock for daylight savings changes** box is also configured correctly on the PC's **Date and Time Properties** screen.

If it should become necessary to modify either of these settings (time zone and/or daylight savings checkbox) on the PC, make the PC adjustments and then reconnect to the device prior to updating the time.

6.8.1 Updating Date and Time Using PC Time

This operation will transfer the date and time of the PC to the device, and will initiate device reboot. The application will adjust the date and time of the PC to UTC prior to sending it to the device.

Prerequisites:

- Verify that the date and time settings of the PC are accurate for the time zone that the PC is configured for on the PC's **Date and Time Properties** screen.
- Verify that **Automatically adjust clock for daylight savings changes** is configured correctly on the **Date and Time Properties** of the PC.

When and where to use:

NOTICE: This setting is necessary for the application to accurately translate the date and time of the PC to UTC. However, it is important to understand that the device does not adjust its UTC time for Daylight Savings Time changes.

Procedure:

1. From the Menu Bar, select **Settings** → **Date & Time**.

   The **Date & Time Configuration** screen appears.

2. Click **Update Date & Time** on the lower portion of the screen.

   The application automatically adjusts the hour to UTC when sending the time to the device.

6.9 Feature Status Window

The **Feature Status** window contains three sections.

Section	Description
Parameters	Displays the Serial Number for the connected device (or allows Serial Number Input when not connected to the device). It also contains fields and buttons used when enabling new features for the device. See Enabling Features with Full Application Connectivity on page 180 and Partial Application Connectivity on page 181 for more information.
Available Features	A grid that displays available features, based on the Entitlement ID displayed in the Parameters section. The grid is labeled **Features in File** if the features are loaded from a previously saved features file. See Partial Application Connectivity on page 181 for more information. There are four fields under **Available Features**: **Feature Name** The name of the feature for which other data on the same row applies. **Total Count** The number of licenses originally secured for the named feature on this Entitlement ID.

Table continued…

	Quantity Available The number of licenses that are still available for the named feature on this Entitlement ID. **Quantity to Activate** Used to enter the number of licenses that you wish to activate for this feature on the connected device. If the Feature Name indicates that the license is a “pack”, or if the name uses other words or numbers to denote more than one, then each license will enable multiple instances of the feature.
Current Features	A grid that displays the status of features currently available for this device. The grid is labeled **Features currently registered to Serial Number** if the current feature list is obtained from the feature licensing server rather than from the device. See Partial Application Connectivity on page 181 for more information. This section consists of three fields: **Feature Name** The name of a device feature. The other columns on the same row provide information regarding the status of the named feature. The feature name displays in either black or blue text. See Enabling Features with Full Application Connectivity on page 180 for more information **Quantity** Shows the current status of the named feature. Zero (0) indicates the feature is not enabled for this device. One (or greater) indicates that some level of feature support is currently enabled. To determine whether the feature is enabled for its maximum allowed capacity, compare **Quantity** with **Maximum Allowed**, as described in the following field. **Maximum Allowed** Shows the maximum allowed capacity of the named feature. When **Maximum Allowed** is equal to **Quantity**, the feature is currently enabled for its maximum capacity. When **Maximum Allowed** is greater than **Quantity**, the feature is not currently enabled for its maximum capacity. The feature capacity can be increased after obtaining an Entitlement ID with available licenses.

6.9.1 Launching the Feature Status Window

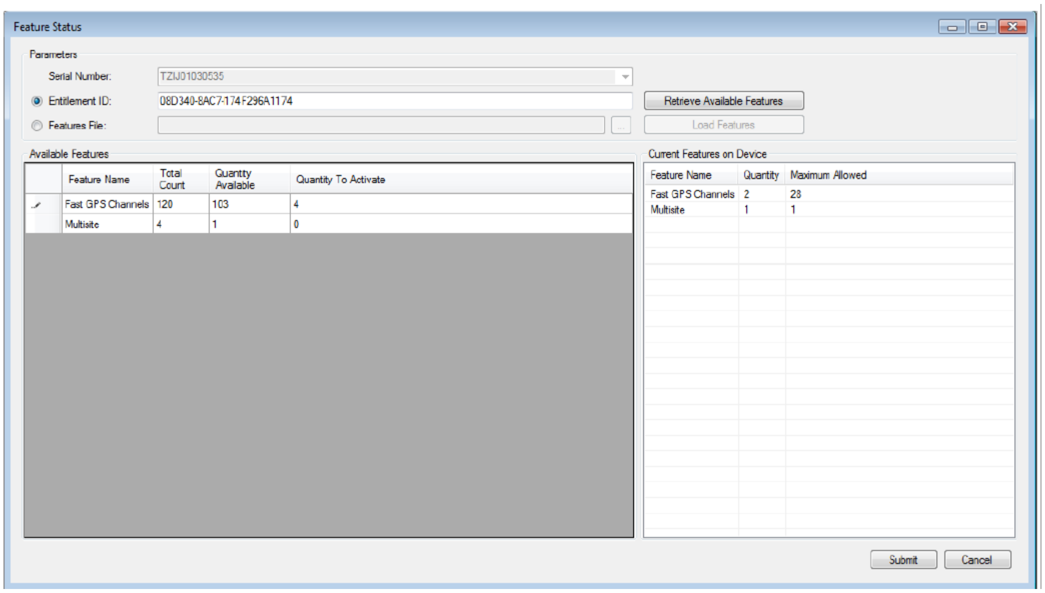
When and where to use: The **Feature Status** window shows the purchasable feature(s) for the connected device, and whether or not any feature on the list is presently enabled. It can also be used to enable additional features for the device.

Procedure:

1. From the Menu Bar, select **Settings** → **Features**.

   The **Feature Status** window appears. The following figure shows the **Feature Status** window with full application connectivity after retrieving available features from a valid Entitlement ID. See Enabling Features with Full Application Connectivity on page 180 for further information.

Figure 63: Feature Status Window



Feature Status

Parameters

Serial Number: TZIJ01030535

● Entitlement ID: 08D340-8AC7-174F296A1174

○ Features File:

Available Features

	Feature Name	Total Count	Quantity Available	Quantity To Activate
	Fast GPS Channels	120	103	4
	Multisite	4	1	0

Current Features on Device

Feature Name	Quantity	Maximum Allowed
Fast GPS Channels	2	28
Multisite	1	1

2 When finished, click **X** or **Cancel** to exit the window.

6.9.2

Viewing Features

Procedure:

1 Launch the **Feature Status** window while connected to the device.

2 View the **Current Features** pane.

Each populated row of Current Features displays the status of one available feature for the connected device. Refer to Feature Status Window on page 177 for more information.

6.9.3

Full Application Connectivity

Full application connectivity is the recommended method to enable features. This method enables features when the application is simultaneously connected to both the device and the feature licensing server and it is recommended because it allows the application to perform important checks that reduce the possibility of user input error.

Whenever the **Feature Status** is screen is launched from the **Menu Bar** while connected to a device, the application attempts to establish communication with the feature licensing server.

If the application detects that there is no connection to the feature licensing server (or some other problem), it displays a message that explains the problem and provides three buttons (**Yes**, **No**, and **Cancel**). Read the message carefully before clicking the most appropriate button to continue.

If the application cannot connect to the feature licensing server, you can view current features, but you cannot enable new features unless you have previously completed the steps outlined in the first sub-section of Partial Application Connectivity on page 181.

IMPORTANT: It is strongly recommended to enable features when there is full application connectivity to both the device and the feature licensing server. If a temporary network problem prevents connection to the feature licensing server, investigate and resolve the connectivity issue. After resolving the connectivity issue, follow the steps outlined in Enabling Features with Full Application Connectivity on page 180.

6.9.3.1

Enabling Features with Full Application Connectivity

Prerequisites:

- Obtain an Entitlement ID that contains one or more licenses for the desired feature(s).
- Connect to the desired device with Administrator Role log-in. The Network Manager must be able to access the internet while connected to the desired device.

When and where to use:

CAUTION: Submitting features as described in this section causes the device to reboot.

Procedure:

1. Launch the **Feature Status** window.
2. Click the **Entitlement ID** field, if not already selected.
3. Copy the Entitlement ID from the source document and paste it into the **Entitlement ID** field.
4. Click the **Retrieve Available Features** button.

   This requires an internet connection and may take a few seconds.

   If the application is able to retrieve information on available features, it loads this information into the **Available Features** pane.
   If the application is not able to retrieve this information, it displays an error message.

5. View the **Available Features** pane.

   Each populated row contains information on a feature available with this Entitlement ID.

6. In **Quantity to Activate**, enter the number of licenses (for the named feature) that you wish to activate for this device. If the Feature Name indicates that the license is a “pack”, or if the name uses other words or numbers to denote more than one, then each license will enable multiple instances of the feature. Take this into account when entering the number of licenses to activate.

   - If the Feature Name is displayed with black text in the **Current Features** pane, then the number of feature instances activated via the **Available Features** pane is added to the number of feature instances displayed in the **Current Features** pane (after submitting the change and completing the operation).
   - If the Feature Name is displayed with blue text in the **Current Features** pane, then the number of feature instances activated via the **Available Features** pane replaces the number of feature instances displayed in the **Current Features** pane (after submitting the change and completing the operation).
   - If the application detects a problem with the number entered into **Quantity to Activate**, it displays an exclamation point icon next to the feature name in the **Available Features** pane. Place the cursor over the icon to view a message with information about the problem.

   If you are enabling multiple features for the connected device from the same Entitlement ID, repeat this step for each desired feature.

7. Click **Submit**.

   All submitted changes must be accepted for any change to be applied

   If a change cannot be accepted, the application displays an error message with information about the problem

If the changes in the **Quantity to Activate** column are accepted, the application provides a reboot warning message. Perform one of the following actions:

- Click **Yes** to apply the changes and reboot the device.
- Click **No** or **Cancel** to abort the operation.

6.9.4 Partial Application Connectivity

This is another alternative method to enable features. However, whenever possible, it is strongly recommended to enable features while the application has full, simultaneous connectivity to both the device and the feature licensing server and by following the steps described in Enabling Features with Full Application Connectivity on page 180.

In some cases the network topology may not allow the application to simultaneously connect to the both the device and the feature licensing server. In this event, enabling features becomes a two part process as described in the following sub-sections. The first part of the process is to connect to the feature licensing server and to create a special features file. The second part is to connect to the desired device, to upload the file, and to submit the features to the device.

6.9.4.1 Connecting to the Features Server and Creating Features Files

The first part of the process is to connect the application to the feature licensing server and to create a special file that can be used to enable features for the device. For this first part of the process, the application must be able to connect to the public internet, but it does not need to connect to the device.

Prerequisites:

- Obtain an Entitlement ID that contains one or more licenses for the desired feature(s).
- Know the Serial Number of the device for which you are enabling the feature.
- Know the type of device for which you are enabling the feature (for example, XRI, XRC or XRT). Not every device type supports every feature.
- The PC should be running the current release version of the MOTOTRBO Connect Plus Network Manager.
- The application must be able to access the internet.

Procedure:

1. Open the **Feature Status** screen when the Network Manager application is running, but not connected to a device.

   Recommended method for launching the application: Locate and double-click the shortcut called **Offline Mode - MOTOTRBO Connect Plus Network Manager**. The shortcut can be accessed via → **All Programs** → **Motorola Solutions**. The Network Manager launches in offline mode.

2. From the Menu Bar, select **Settings** → **Features**.

   The application attempts to automatically connect to the feature licensing server. If the application cannot connect to the feature licensing server, a message is displayed. In that event, the steps described in this sub-section cannot be performed until the connectivity problem is resolved.

3 In the **Serial Number** field, enter the Serial Number of the device on which the features should be enabled.

IMPORTANT: Enter the Serial Number carefully. The application is not able to perform validation on the entered number. Entering a Serial Number (and then subsequently saving to a features file) incorrectly will require Customer Service to correct the license.

- When entering a Serial Number from the keyboard, alpha characters should be entered as upper case.
- As an alternative, select the desired serial number from the drop down list, if applicable. (If this copy of the application has previously connected to a device, its serial number is displayed in a drop-down list.)

4 Click **Get Currently Registered Features**.

If there are any features currently registered in the feature licensing server for the inputted serial number, they will be displayed in the in the panel called **Features currently registered to Serial Number**. For more information on the columns in this panel, see Viewing Features on page 179.

Any features activated on the device associated with this serial number prior to Connect Plus System Release 1.6 (and not recorded on the Feature Licensing server) will not display in Features currently registered to Serial Number.

5 Perform one of the following actions:

- If using an Entitlement ID to add new features, go to step 6.
- If creating a file that can be used to restore the currently registered features of the device only, go to step 9.

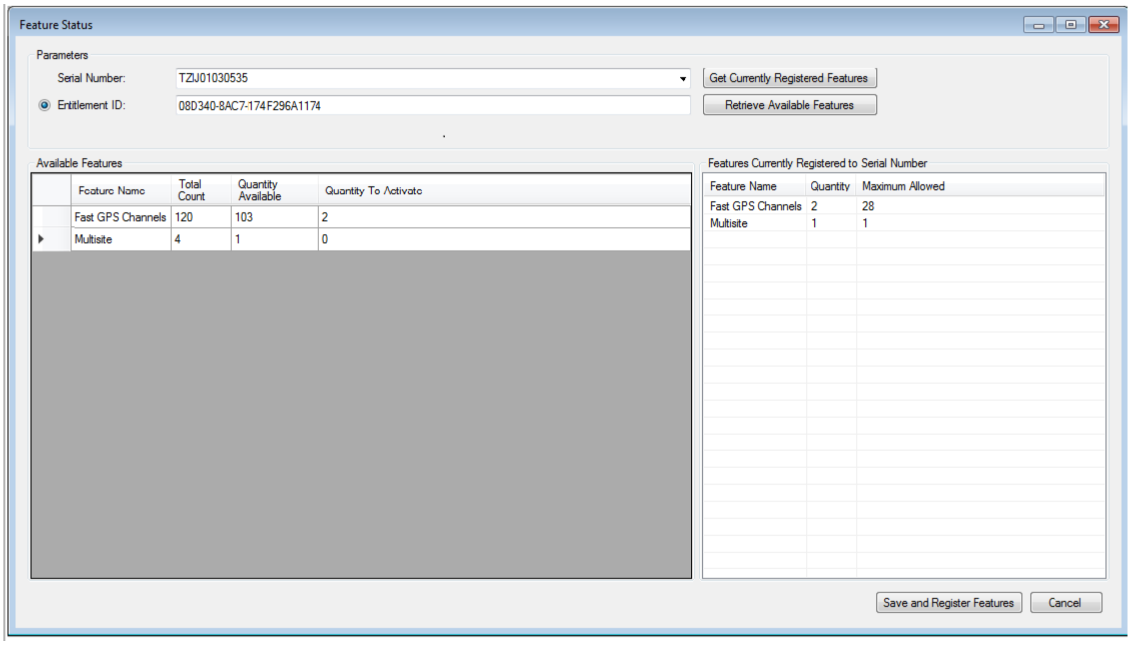
6 Copy the Entitlement ID from the source document and paste it into the **Entitlement ID** field.

7 Click **Retrieve Available Features**.

This requires an internet connection and may take a few seconds.

The application will retrieve information on available features. If the application is able to retrieve information on available features, it loads this information into the **Available Features** pane. If the application is not able to retrieve this information, it displays an error message. The following image shows the **Feature Status** screen in offline mode after retrieving available features. Each populated row of Available Features contains information on a feature available with this Entitlement ID.

Figure 64: Features Screen in Offline Mode



Feature Status
Parameters
Get Currently Registered Features
Retrieve Available Features
Available Features
Features Currently Registered to Serial Number
Save and Register Features
Cancel

Serial Number: TZIJ01030535

● Entitlement ID: 08D340-8AC7-174F296A1174

Available Features

Feature Name	Total Count	Quantity Available	Quantity To Activate
Fast GPS Channels	120	103	2
Multisite	4	1	0

Features Currently Registered to Serial Number

Feature Name	Quantity	Maximum Allowed
Fast GPS Channels	2	28
Multisite	1	1

8 In **Quantity to Activate**, enter the number of licenses (for the named feature) that you wish to activate for the device that corresponds to the entered Serial Number.

If the Feature Name indicates that the license is a “pack”, or if the name uses other words or numbers to denote more than one, then each license will convert to multiple instances of the feature when creating the features file (as described in a subsequent step). Take this into account when entering the number of licenses to activate.

If the application detects a problem with the number entered into Quantity to Activate, it displays an exclamation point icon next to the feature name in the **Available Features** pane. Place the cursor over the icon to view a message with information about the problem.

9 Click **Save and Register Features**.

This launches the **Save As** file dialogue, with a default file name and directory. It is recommended to use these defaults, but the file name and/or directory can be changed if necessary.

10 Make a record of the file name and directory (for future reference).

The saved file will be used to activate features on the device, as described in the next sub-section.

11 Click the **Save** button in the file dialogue.

The application conducts some checks. If the application does not encounter any problems, it displays a message advising that the features will be activated on the server.

12 Perform one of the following actions:

- To proceed, click **Yes**.
- To abort the operation, click **No** or **Cancel**.

13 When finished, click the **X** to close the application.

6.9.4.2

Connecting to the Device and Uploading the Features File

The second part of the process is to connect the application to the desired device, to upload the features file, and to submit (activate) the features.

Prerequisites:

- Obtain the features file that was created in the process described in the previous sub-section. The file can only be used with that the device whose Serial Number matches the Serial Number that was inputted when the file was created.
- Connect to the desired device with Administrator Role log-in.
- Launch the **Feature Status** window.

When and where to use:

WARNING: Submitting features as described in this section causes the device to reboot.

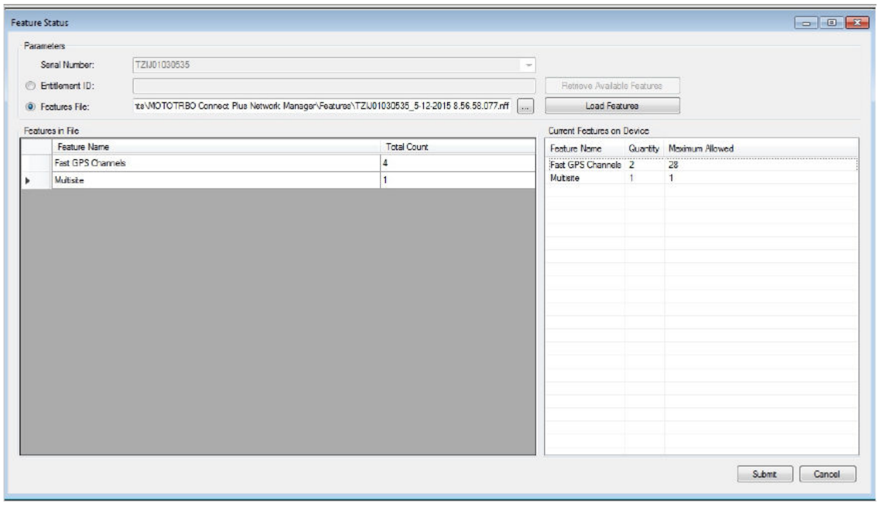
Procedure:

1. Click the **Features File** bullet, if not already selected.
2. Click the **Browse** icon to launch the **Select a Features File** file dialogue.
3. Locate and select the previously saved features file (that was created for the Serial Number that matches the connected device) and click **Open**.

   The path and file name displays in the **Features File** field.

4. Click **Load Features**.

   The features listed in the saved file are displayed in the **Features in File** pane as shown in the following image.



Feature Status

Parameters

Serial Number: TZIJ01030535

○ Entitlement ID:

● Features File: :ts\MOTOTRBO Connect Plus Network Manager\Features\TZIJ01030535_5-12-2015 8.56.58.077.nff

Features in File

Feature Name	Total Count
Fast GPS Channels	4
Multisite	1

Current Features on Device

Feature Name	Quantity	Maximum Allowed
Fast GPS Channels	2	28
Multisite	1	1

   Each populated row displays information on a feature:

   Feature Name
   The name of the feature for which other data on the same row applies.

   Total Count
   The total number of instances of the named feature that will be enabled in the device after submitting the change.

5. Click **Submit**.

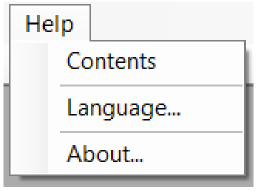
6 Perform one of the following actions:

- To apply the changes and reboot the device, click **Yes**.
- To abort the operation, click **No** or **Cancel**.

6.10 Application Help Menu

This application comes with a Help file. The Help file is accessible from the **Help** menu.

Figure 65: Help Menu Drop Down Menu



6.10.1 Launching the Application Help File

Procedure:

1 Click on **Help** in the **Menu** Bar.

2 Click on **Contents …** within the menu.

The default web browser displays the Help page in a new tab.

6.10.2 Selecting the Application Display Language

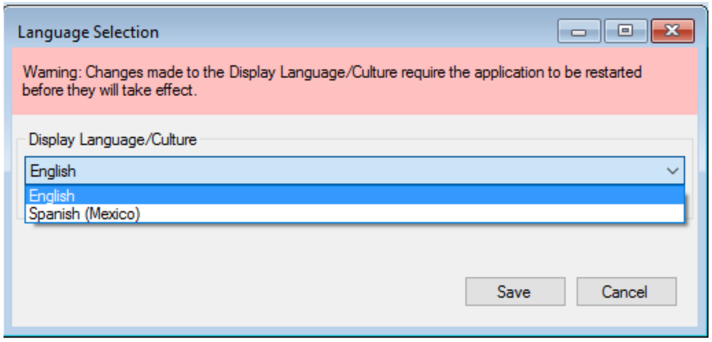
When and where to use: The application can be configured to display in English, or in the same language as the Operating System of the computer (if other than English and supported by the application).

Procedure:

1 From the Menu Bar, select **Help** → **Language ....**

The **Language Selection** screen appears.

Figure 66: Language Selection Screen



Language Selection

Warning: Changes made to the Display Language/Culture require the application to be restarted before they will take effect.

Display Language/Culture: English

2 Click the arrow under **Display Language/Culture**.

The application displays a list of one or two languages.

NOTICE: For some computers, English is the only available language.

3. Select the desired Language/Culture from the list and click **Save**.
4. Manually close and then re-start the application to enforce the language change immediately.

   NOTICE: The language change is automatically communicated to the Network Manager application the next time it is launched by the Network Manager Connection Tool.

Postrequisites: Changes to the Display Language/Culture require the application to be manually re-started before the changes take effect.

6.10.3 Launching the About Screen

Procedure:

1. Click **Help** in the **Menu** Bar.
2. Click **About…** within the menu.

   The **About** window displays software version information and copyright information.

Chapter 7

Appendix A Determining the UPS Capacity

Procedure:

1. List all equipment to be protected by the UPS.
2. Write down the voltage and amperage for each device.
3. Multiply the voltage by the amperage of each device to calculate the Volt/Amps (VA).

   NOTICE: Some equipment may be marked with a power consumption measured in Watts. To convert Watts to VA, divide Watts by 0.65 (for a power factor of 0.65), or multiply by 1.54. The power factor refers to the relationship between the apparent power (volt-amps) required by the device and the actual power (watts) produced by the device.
4. Total the VA for all devices you want to protect with the UPS.
5. Multiply the subtotal found in Step 4 by 0.25. This number takes into account room for future growth. This growth factor allows for a 5% rate of growth for each year over a five-year period.
6. Add the results of steps 4 and 5 to get the Required VA. Now you can select the appropriate UPS model by choosing a model that has a VA rating at least as large as the Required VA that you calculated.

This page intentionally left blank.