

System Release 2.8
MOTOTRBO™ Connect Plus



XRT Gateway User Guide

JUNE 2017

68012005028–GC

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.

© 2017 Motorola Solutions, Inc. All Rights Reserved

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
68012005028–GC	Original release of the <i>XRT Gateway User Guide</i> for MOTOTRBO™ Connect Plus	June 2017

This page intentionally left blank.

Contents

Copyrights	3
Contact Us	5
Declaration of Conformity	7
Document History	9
List of Figures	17
List of Procedures	19
Commercial Warranty	23
Limited Warranty.....	23
MOTOROLA COMMUNICATION PRODUCTS.....	23
What This Warranty Covers and For How Long.....	23
General Provisions.....	23
State Law Rights.....	23
How to Get Warranty Service.....	23
What This Warranty Does Not Cover.....	23
Patent and Software Provisions.....	24
Governing Law.....	25
Computer Software Copyrights.....	25
Open Source Software Legal Notices.....	25
About the XRT Gateway User Guide	27
What Is Covered in This Guide.....	27
Helpful Background Information.....	27
Related Information.....	27
Chapter 1: Introduction	29
1.1 MOTOTRBO Connect Plus XRT Configuration Tool.....	30
Chapter 2: Safety Information	31
2.1 Electrical.....	31
2.1.1 Grounding.....	31
2.2 Servicing.....	31
2.3 Regulatory.....	31
2.3.1 FCC Compliance — Radio Frequency Interference.....	31
2.3.2 Other.....	32
2.3.2.1 Network Connected Equipment.....	32
2.3.2.2 Lithium Battery Warning.....	32
2.3.2.3 Cable Connections.....	32
Chapter 3: System Planning	33

3.1 Talk Path Capacity.....	33
3.2 Simultaneous Calls Capacity.....	33
3.3 Network Site Capacity.....	33
3.3.1 Connect Plus Release 1.6.....	33
3.3.2 Network Planning Bandwidth Considerations.....	33
Chapter 4: Installation.....	35
4.1 Unpacking and Checking Equipment.....	35
4.2 Initial Power Up.....	35
4.2.1 Power Requirements.....	35
4.2.2 Fuse.....	35
4.2.3 Connecting the Power Cable.....	36
4.2.4 On/Off Switch.....	36
4.3 Getting Acquainted with the 9100 Model.....	36
4.3.1 Front Panel.....	37
4.3.1.1 Front Panel Photo.....	37
4.3.1.2 Indicators.....	37
4.3.2 Rear Panel.....	38
4.3.2.1 Rear Panel Photo.....	39
4.3.2.2 Ports.....	39
4.4 System Connections.....	41
4.4.1 XRT Connected to a Connect Plus Network.....	41
4.4.2 PC Connection for Initial Configuration.....	42
4.4.2.1 Ethernet Port Connection of the Device.....	42
4.4.2.2 Direct Connection: PC to Device.....	43
4.4.3 Power Recommendations.....	44
4.4.3.1 Primary Power Source.....	44
4.4.3.2 Backup Power Source.....	44
4.4.4 Mounting the Device in a Rack.....	45
Chapter 5: Communicating with the Device.....	49
5.1 Configuring the PC Network for Initial Configuration.....	49
5.2 MOTOTRBO Connect Plus XRT Configuration Tool Software.....	49
5.2.1 Installing MOTOTRBO Connect Plus XRT Configuration Tool Software on the PC.....	50
5.2.2 Launching the MOTOTRBO Connect Plus XRT Configuration Tool.....	50
5.2.3 Establishing Connection with the Device.....	51
5.2.3.1 Configuring the Socket Connection.....	51
5.2.3.2 Configuring the Serial Connection.....	51
5.2.3.3 Logging Into the Device.....	51
Chapter 6: Site and Network Configuration.....	53

6.1 Critical Settings Configuration.....	53
6.1.1 Rebooting the Device Now.....	53
6.1.2 Rebooting the Device Later.....	54
6.1.3 Indications of Pending Reboot.....	54
6.2 Configuring Network Settings.....	54
6.2.1 Redundant XRT Gateway Capability.....	55
6.2.2 XRT Gateway Role and Network Settings.....	56
6.2.2.1 Network Settings: LAN 1 Network.....	56
6.2.2.2 Network Settings: LAN 2 Network.....	57
6.3 Configuring Site Settings.....	58
6.3.1 Site Settings - Critical (Left Pane).....	58
6.3.1.1 Site Configuration Parameters.....	59
6.3.1.2 Network Configuration Parameters.....	60
6.3.1.3 NTP Configuration Parameters.....	61
6.3.2 Site Settings - Non-Critical.....	63
6.3.2.1 Call Configuration Parameters.....	63
6.4 Configuring for Multisite (Multisite Networks Only).....	65
6.4.1 Multisite Settings.....	66
6.4.1.1 Saving Changes to the Multisite Configuration Screen.....	66
6.4.1.2 Discarding Changes to the Multisite Configuration Screen.....	66
6.4.1.3 Connect Plus Network ID.....	67
6.4.1.4 Site ID.....	67
6.4.1.5 Site Alias.....	67
6.4.1.6 Global IP Address.....	67
6.4.1.7 Global TCP Port.....	68
6.4.1.8 Notes.....	68
Chapter 7: System Management.....	69
7.1 Provisioning and Configuring XRT Subscribers.....	69
7.1.1 Initial XRT Integration in the Connect Plus Network.....	69
7.1.1.1 User Registry Window.....	71
7.1.2 User Details.....	72
7.1.2.1 Radio ID.....	72
7.1.2.2 Alias.....	73
7.1.2.3 Record Status.....	73
7.1.2.4 Priority.....	73
7.1.2.5 Serial Number.....	73
7.1.2.6 Multigroup ID.....	74
7.1.2.7 Registration Authentication.....	74
7.1.2.8 Default Emergency Revert Group.....	76

7.1.3 User Details Check Boxes.....	76
7.1.3.1 Site All Call Voice Init.....	77
7.1.3.2 Authorizing Private Call Init.....	78
7.1.3.3 Authorizing Private Call Receive.....	78
7.1.3.4 Enabling Packet Data Call.....	78
7.1.3.5 Enabling Generic Data Call.....	78
7.1.3.6 Enabling Confirmed Transmission.....	78
7.1.3.7 Authorizing Remote Monitor Init.....	78
7.1.3.8 Authorizing Remote Monitor Receive.....	79
7.1.3.9 Authorizing Disable Command Init.....	79
7.1.3.10 Authorizing Disable Command Receive.....	79
7.1.3.11 Authorizing Enable Command Init.....	79
7.1.3.12 Authorizing Enable Command Receive.....	79
7.1.3.13 Authorizing Multigroup Call Init.....	79
7.1.3.14 Authorizing Radio Check Init.....	79
7.1.3.15 Authorizing a Call Alert Init.....	80
7.1.3.16 Authorizing Emergency Init.....	80
7.1.3.17 Notes.....	80
7.1.4 Group Details Screen.....	80
7.1.4.1 Group ID.....	80
7.1.4.2 Alias.....	81
7.1.4.3 Record Status.....	81
7.1.4.4 Priority.....	81
7.1.4.5 Allowing Phone Access.....	81
7.1.4.6 Priority Monitor.....	81
7.1.4.7 Notes.....	82
7.1.5 Multigroup Details.....	82
7.1.5.1 Multigroup ID.....	82
7.1.5.2 Alias.....	82
7.1.5.3 Record Status.....	83
7.1.5.4 Priority.....	83
7.1.5.5 Allowing Phone Access.....	83
7.1.5.6 Priority Monitor.....	83
7.1.5.7 Notes.....	83
7.1.6 Site All Call Details.....	84
7.1.6.1 Enabling Priority Monitor.....	84
7.1.7 Creating Subscriber/Group/Multigroup Records.....	84
7.1.7.1 Submenu Bar for Records Creation.....	84
7.1.8 Locating Subscriber/Group/Multigroup Records.....	86

7.1.8.1 Using the Submenu Bar Find Tools.....	86
7.1.9 Deleting Subscriber/Group/Multigroup Records.....	87
7.1.9.1 Submenu Bar for Deleting Records.....	87
7.2 Site Access and Permanent Registration.....	88
7.2.1 Launching the Site Access and Permanent Registration Screen.....	90
7.2.2 Entering IDs.....	90
7.2.3 Configuring a List of Restricted Radios (SUs) for a Specific Site.....	91
7.2.4 Configuring a List of Restricted Talk Groups for a Specific Site.....	92
7.2.5 Configuring a List of Permanently Registered Talk Groups for a Specific Site.....	92
7.2.6 Configuring a List of Restricted Sites for a Specific Radio.....	93
7.2.7 Configuring a List of Restricted Sites for a Specific Talk Group ID.....	94
7.2.8 Configuring a List of Permanently Registered Sites for a Specific Talk Group ID...	96
7.3 Backup/Restore Utility.....	97
7.3.1 Saving a Site Configuration and User Records to a File.....	97
7.3.2 Restoring a Site Configuration from a File.....	98
7.3.2.1 User Health Tool.....	98
7.4 Site Control.....	99
7.4.1 Rebooting a Site.....	99
7.4.2 Uploading/Upgrading Device Firmware.....	100
7.4.2.1 Uploading the Firmware File.....	101
7.4.2.2 Removing a Firmware File.....	101
7.4.2.3 Upgrading the Firmware.....	101
7.4.3 Site Status Window.....	102
7.4.3.1 Determining Connected Sites and Registered Units.....	102
7.4.4 Changing a Password.....	103
7.4.5 Switching to	103
7.4.6 Uploading a Properties Change File.....	104
7.5 Alerts and Alarms Management.....	104
7.5.1 Overview.....	104
7.5.2 Launching the Alerts/Alarms Management Window.....	105
7.5.2.1 XRT Gateway Alerts.....	105
7.5.2.2 Refreshing the Alerts Window.....	106
7.5.3 Alert Notifications (Email).....	106
7.5.3.1 Creating Alert Notification Groups.....	107
7.5.4 Setting Up SMTP for Email Notifications.....	108
7.6 Logs.....	109
7.6.1 Event Log Viewer.....	109
7.6.1.1 Event Logs.....	110
7.7 Feature Status Window.....	112

7.7.1 Launching the Feature Status Window.....	113
7.7.2 Viewing Features.....	114
7.7.3 Full Application Connectivity.....	114
7.7.3.1 Enabling Features with Full Application Connectivity.....	115
7.7.4 Partial Application Connectivity.....	116
7.7.4.1 Connecting to the Features Server and Creating Features Files.....	116
7.7.4.2 Connecting to the Device and Uploading the Features File.....	118
7.8 Date Time Configuration.....	119
7.8.1 Launching the Date Time Configuration Window.....	120
7.8.2 Updating Date and Time Using PC Time.....	120
7.9 XRT Configuration Tool Multiple Windows Display Options.....	121
7.9.1 Cascading Windows.....	121
7.9.2 Tiling Windows Horizontally.....	122
7.9.3 Tiling Windows Vertically.....	122
7.10 XRT User Configuration.....	123
7.10.1 Creating a New User.....	123
7.10.2 Entering User Details.....	124
7.11 Application Help Menu.....	125
7.11.1 Launching the Application Help File.....	126
7.11.2 Selecting the Application Display Language.....	126
7.11.3 Launching the About Screen.....	127
Chapter 8: Appendix A Determining the UPS Capacity.....	129

List of Figures

Figure 1: Fuse.....	36
Figure 2: Power Input Connector.....	36
Figure 3: XRT 9100 Front Panel.....	37
Figure 4: Power LED.....	37
Figure 5: Storage Activity LED.....	37
Figure 6: Ethernet Activity LEDs.....	38
Figure 7: Serial Activity LEDs.....	38
Figure 8: Rear Panel of XRT 9100.....	39
Figure 9: Video (VGA) Port.....	39
Figure 10: PS/2 Port.....	39
Figure 11: The 9100 model Universal Serial Bus (USB).....	40
Figure 12: Ethernet Ports.....	40
Figure 13: RS-232/422/485 Serial Ports (P1-P2).....	40
Figure 14: RS-485 Serial Ports (P3-P8).....	41
Figure 15: Grounding Connection.....	41
Figure 16: Connecting the XRT to a Connect Plus Network.....	42
Figure 17: XRT 9100 Gateway Connection to Ethernet Switch.....	43
Figure 18: LAN Cable for PC Connection.....	43
Figure 19: Null Modem Cable.....	44
Figure 20: Primary Power Source.....	44
Figure 21: Reboot Warning Prompt.....	53
Figure 22: Gateway Role and Network Settings Screen.....	55
Figure 23: Critical Settings Configuration Screen.....	59
Figure 24: Multisite Configuration Window.....	66
Figure 25: User Registry Window.....	71
Figure 26: User Details Screen.....	72
Figure 27: Serial Number Warning.....	74
Figure 28: User Details Check Boxes Screen.....	77
Figure 29: Group Details Screen.....	80
Figure 30: Multigroup Details Screen.....	82
Figure 31: Site All Call Details Screen.....	84
Figure 32: Icons Within the Submenu Bar.....	84
Figure 33: Current List.....	94
Figure 34: Backup and Restore Utility Window.....	97
Figure 35: User Health Tool Screen.....	99
Figure 36: Site Status Window.....	102

Figure 37: Alerts/Alarms Management Option in the Drop Down Menu.....	105
Figure 38: Alert Management Window.....	107
Figure 39: Event Log Viewer Window.....	109
Figure 40: Example of Feature Status Window	114
Figure 41: Features Screen in Offline Mode.....	117
Figure 42: Date Time Configuration Screen.....	120
Figure 43: Cascaded Windows.....	121
Figure 44: Windows Tiled Horizontally.....	122
Figure 45: Windows Tiled Vertically.....	123
Figure 46: User Configuration Screen.....	124
Figure 47: Help Menu Drop Down Menu.....	125
Figure 48: Language Selection Screen.....	126

List of Procedures

Unpacking and Checking Equipment	35
Connecting the Power Cable	36
Connecting to the Device Through an Ethernet Switch	43
Connecting Through the Serial Port of the Device	44
Mounting the Device in a Rack	45
Configuring the PC Network for Initial Configuration	49
Installing MOTOTRBO Connect Plus XRT Configuration Tool Software on the PC	50
Launching the MOTOTRBO Connect Plus XRT Configuration Tool	50
Configuring the Socket Connection	51
Configuring the Serial Connection	51
Logging Into the Device	51
Rebooting the Device Now	53
Rebooting the Device Later	54
Configuring Network Settings	54
Entering the Primary IP Address	56
Entering the Secondary IP Address	57
Entering the IP Mask (Netmask)	57
Entering the Gateway (Router) IP Address	57
Entering the Domain Name Server(s)	57
Entering the Primary IP Address	57
Entering the Secondary XRT Gateway IP Address	58
Configuring Site Settings	58
Entering the NTP Server Address	62
Allowing Connection From Bridge	63
Configuring for Multisite (Multisite Networks Only)	65
Saving Changes to the Multisite Configuration Screen	66
Discarding Changes to the Multisite Configuration Screen	66
Launching the User Registry Window	71
Enabling Physical Serial Number Authentication	75
Entering the Physical Serial Number	75
Authorizing Private Call Init	78
Authorizing Private Call Receive	78
Enabling Packet Data Call	78
Enabling Generic Data Call	78
Enabling Confirmed Transmission	78
Authorizing Remote Monitor Init	78

Authorizing Remote Monitor Receive	79
Authorizing Disable Command Init	79
Authorizing Disable Command Receive	79
Authorizing Enable Command Init	79
Authorizing Enable Command Receive	79
Authorizing Multigroup Call Init	79
Authorizing Radio Check Init	79
Authorizing a Call Alert Init	80
Authorizing Emergency Init	80
Allowing Phone Access	81
Allowing Phone Access	83
Enabling Priority Monitor	84
Creating a New Subscriber Unit	85
Canceling a New User Record	85
Creating a New Group	85
Creating a New Multigroup	85
Canceling A New Group/Multigroup Record	86
Searching Records Using the Find Icon	86
Searching Records via the Text Box	87
Deleting a Subscriber Unit	88
Deleting a Group	88
Deleting a Multigroup	88
Launching the Site Access and Permanent Registration Screen	90
Entering IDs	90
Configuring a List of Restricted Radios (SUs) for a Specific Site	91
Configuring a List of Restricted Talk Groups for a Specific Site	92
Configuring a List of Permanently Registered Talk Groups for a Specific Site	92
Configuring a List of Restricted Sites for a Specific Radio	93
Configuring a List of Restricted Sites for a Specific Talk Group ID	94
Configuring a List of Permanently Registered Sites for a Specific Talk Group ID	96
Saving a Site Configuration and User Records to a File	97
Restoring a Site Configuration from a File	98
Rebooting a Site	99
Uploading/Upgrading Device Firmware	100
Uploading the Firmware File	101
Removing a Firmware File	101
Upgrading the Firmware	101
Determining Connected Sites and Registered Units	102
Changing a Password	103

Switching to ...	103
Uploading a Properties Change File	104
Launching the Alerts/Alarms Management Window	105
Refreshing the Alerts Window	106
Creating Alert Notification Groups	107
Setting Up SMTP for Email Notifications	108
Downloading Events	110
Clearing Remote Logs	110
Saving to Disk	110
Loading an Archive File	111
Deleting an Archived File	111
Filtering Events	112
Launching the Feature Status Window	113
Viewing Features	114
Enabling Features with Full Application Connectivity	115
Connecting to the Features Server and Creating Features Files	116
Connecting to the Device and Uploading the Features File	118
Launching the Date Time Configuration Window	120
Updating Date and Time Using PC Time	120
Cascading Windows	121
Tiling Windows Horizontally	122
Tiling Windows Vertically	122
Creating a New User	123
Entering User Details	124
Launching the Application Help File	126
Selecting the Application Display Language	126
Launching the About Screen	127
Appendix A Determining the UPS Capacity	129

This page intentionally left blank.

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:

XRT 9000 Gateway	Two (2) Years
XRT 9100 Gateway	Two (2) Years

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 XRT Gateway User Guide

This User Guide provides installation and operation instructions for the MOTOTRBO™ Connect Plus XRT Gateway.

What Is Covered in This Guide

The *XRT Gateway User Guide* contains the following chapters:

- [Introduction on page 29](#)
- [Safety Information on page 31](#)
- [System Planning on page 33](#)
- [Installation on page 35](#)
- [Communicating with the Device on page 49](#)
- [Site and Network Configuration on page 53](#)
- [System Management on page 69](#)

In addition, this guide contains [Appendix A Determining the UPS Capacity on page 129](#).

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
<i>Standards and Guidelines for Communication Sites</i> (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

Thank you for choosing the Motorola Solutions XRT Gateway. XRT is designed to perform protocol translation for equipment and applications wishing to interact with the MOTOTRBO™ Connect Plus digital trunking system. The XRT is the original Gateway hardware platform.

XRT is an Internet Protocol (IP) based device that allows connectivity from authorized clients that are part of the Motorola Solutions Application Development Partner (ADP) Program. The XRT Application Protocol Interface (API) is a published document available to all Motorola Solutions Application Development Partners. The XRT Gateway Protocol Specification defines the messages that provide access to the following features:

- Multigroup Call
- Network Wide All Call initiated by an XRT Client
- Private Call
- Emergency Call
- Notification of Emergency Alert sent by Connect Plus SU
- Call Alert
- Radio Monitor
- Airtime Billing (including Fast GPS Historical Data)
- Radio Check
- Radio Enable
- Radio Disable
- Packet Data Call
- Redundant XRT Gateway (free option upon purchasing second XRT Gateway per XRT site)
- Fault Management with automatic email notification
- Generic Data Call
- Configuration Service: When the feature permission is enabled in the XRT Gateway, an authorized XRT Client can remotely configure certain settings in XRC Controller sites via the XRT

When the client application establishes communication with the XRT, messages must be exchanged to identify the client, to check authorization, and to determine client privileges. Client privileges, which are configured into the XRT, include access to airtime billing information from the Connect Plus network and the ability to register Talk Paths and/or Data Paths with the XRT. Group Talk Paths support group communications with Connect Plus radios. Private Talk paths support individual communications, such as Private Calls, Radio Check, etc. Data Paths support the ability to initiate and receive packet data calls. The total number of Talk Paths and Data Paths registered by all clients cannot exceed the number of Talk Paths licensed for that XRT, which is a maximum of 750 for the XRT 9100. The number of licensed Talk Paths determines how many Group and Private IDs can be registered by all clients, but not the maximum number of simultaneous calls. The maximum number of simultaneous calls on a single XRT 9100 is 100. This total includes voice calls and non-voice calls (Call Alert, Radio Check, Enable, Disable etc). Packet Data Calls do not count against the limit for simultaneous calls.

1.1

MOTOTRBO Connect Plus XRT Configuration Tool

MOTOTRBO Connect Plus XRT Configuration Tool is the software application used to configure the configurable settings of the XRT.

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

Electrical

2.1.1

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.

2.2

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.

2.3

Regulatory

2.3.1

FCC Compliance — Radio Frequency Interference

The Federal Communications Commission (in 47 CFR Part 15 subpart A) has specified that the following notice be brought to the attention of the users of this product.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at the expense of the user.

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

2.3.2

Other

2.3.2.1

Network Connected Equipment

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

2.3.2.2

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.

2.3.2.3

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.

Chapter 3

System Planning

3.1

Talk Path Capacity

The number of Talk Paths which includes Group Talk Paths and Private Talk Paths that can be registered by all clients to a single device is determined by the number of Talk Paths licensed for that device. The number of Talk Paths that can be registered is up to a maximum of 750 for XRT 9100.

3.2

Simultaneous Calls Capacity

The number of simultaneous calls that can occur on a single XRT 9100 is 100 calls. This total includes voice calls and non-voice calls like Call Alert, Radio Check, Enable, Disable, and more.

3.3

Network Site Capacity

3.3.1

Connect Plus Release 1.6

Connect Plus release version 1.6 supports a maximum of 250 RF sites (site numbers 1-250) and a maximum of five (5) XRT Gateways (site numbers 251-255) on a Connect Plus multisite network.

3.3.2

Network Planning Bandwidth Considerations

Careful consideration should be given to bandwidth requirements for the XRT. During the planning phase of installation, please reference the Motorola *MOTOTRBO Connect Plus System Planner* for detailed discussion and calculation tools.

This page intentionally left blank.

Chapter 4

Installation



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

4.1

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.

4.2

Initial Power Up

4.2.1

Power Requirements

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

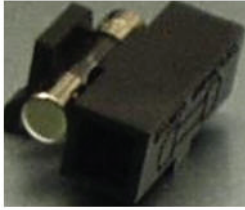
4.2.2

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



4.2.3

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



4.2.4

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.

4.3

Getting Acquainted with the 9100 Model

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

4.3.1

Front Panel

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

4.3.1.1

Front Panel Photo

The following image shows the Front Panel of the XRT 9100 Gateway.

Figure 3: XRT 9100 Front Panel



4.3.1.2

Indicators

4.3.1.2.1

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 is turned to the on position.

Figure 4: Power LED



4.3.1.2.2

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 5: Storage Activity LED



4.3.1.2.3

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.

4.3.1.2.4

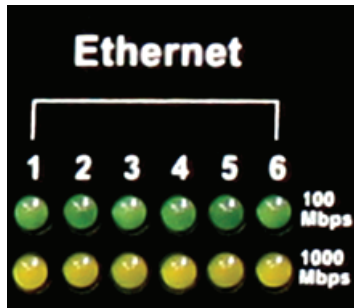
Ethernet Activity LEDs

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 6: Ethernet Activity LEDs



4.3.1.2.5

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 7: Serial Activity LEDs



4.3.1.2.6

Programmable LEDs

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

4.3.2

Rear Panel

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

4.3.2.1

Rear Panel Photo

The following image shows the rear panel of the device.

Figure 8: Rear Panel of XRT 9100



4.3.2.2

Ports

4.3.2.2.1

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 9: Video (VGA) Port



4.3.2.2.2

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 10: PS/2 Port



4.3.2.2.3

Universal Serial Bus (USB)

Two USB ports are located on the left side of the rear panel and to the right of the PS/2 port. The USB ports are used for memory expansion, where applicable.

Figure 11: The 9100 model Universal Serial Bus (USB)

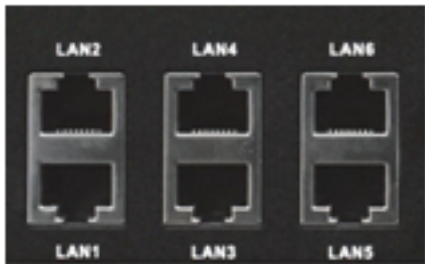


4.3.2.2.4

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 12: Ethernet Ports



4.3.2.2.5

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

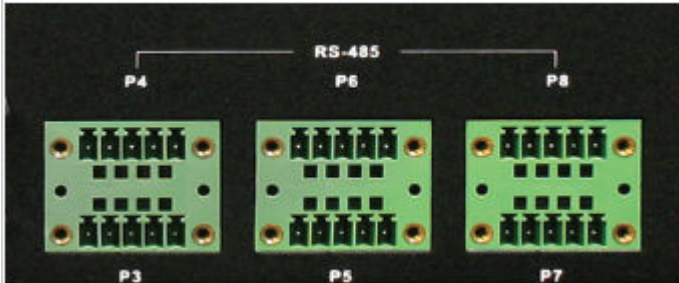


4.3.2.2.6

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 14: RS-485 Serial Ports (P3-P8)



4.3.2.2.7

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 15: Grounding Connection



4.4

System Connections

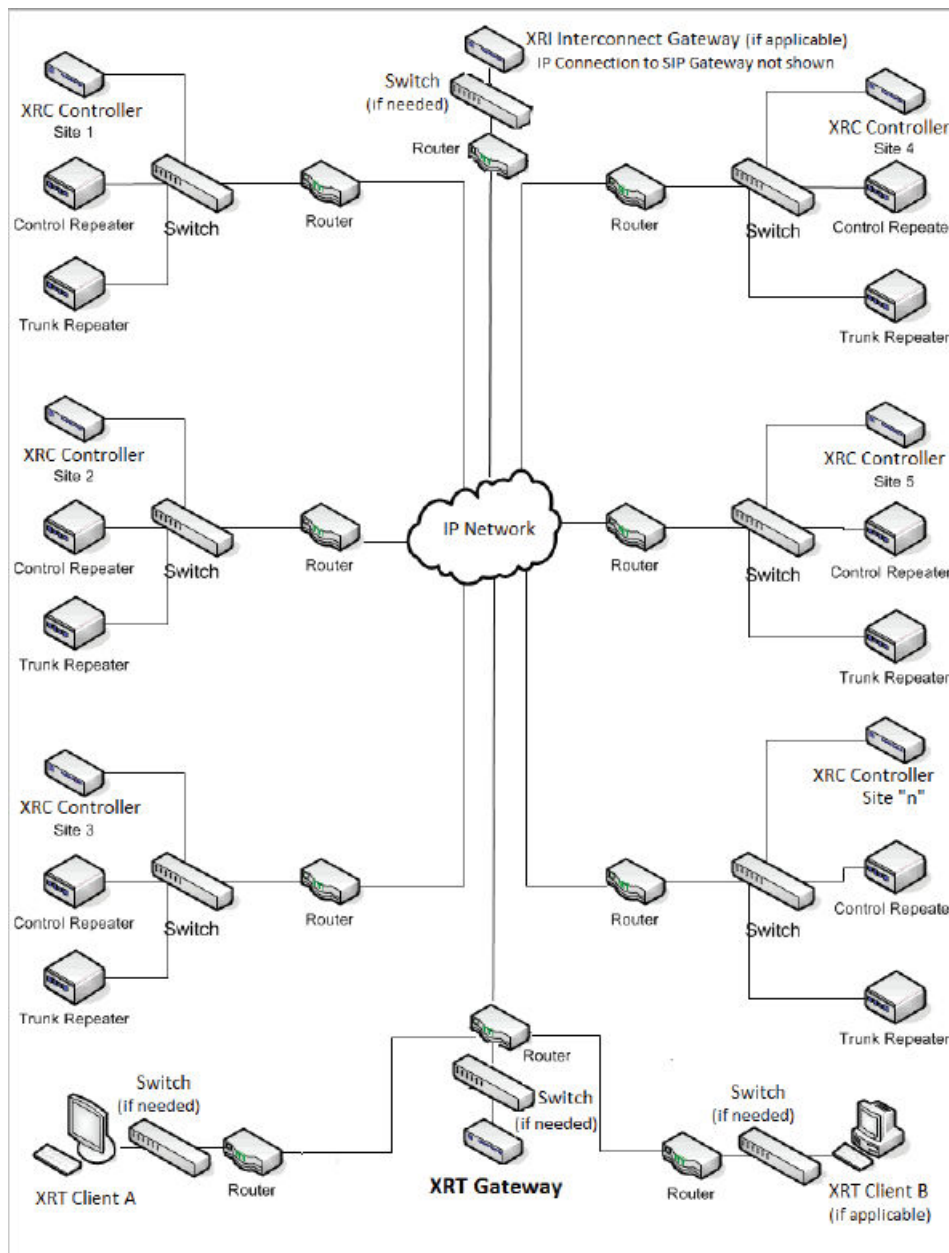
This section describes how to connect the device into a Connect Plus system.

4.4.1

XRT Connected to a Connect Plus Network

The following figure provides a general overview of Connect Plus network hardware. The figure is provided as example and is not representative of every network or topology. The XRC, XRT, and XRI do not currently support multicast IP traffic. The System Administrator must design or configure the IP network such a way that no multicast messages are sent to the XRC, XRT or XRI. The XRT and XRT Client can be co-located, if desired, as long as this important guideline is followed.

Figure 16: Connecting the XRT to a Connect Plus Network



4.4.2 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 42](#)
- [Connecting Through the Serial Port of the Device on page 44](#)

4.4.2.1 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 42](#).

4.4.2.1.1

Connecting to the Device Through an Ethernet Switch

Prerequisites: Minimum switch requirements:

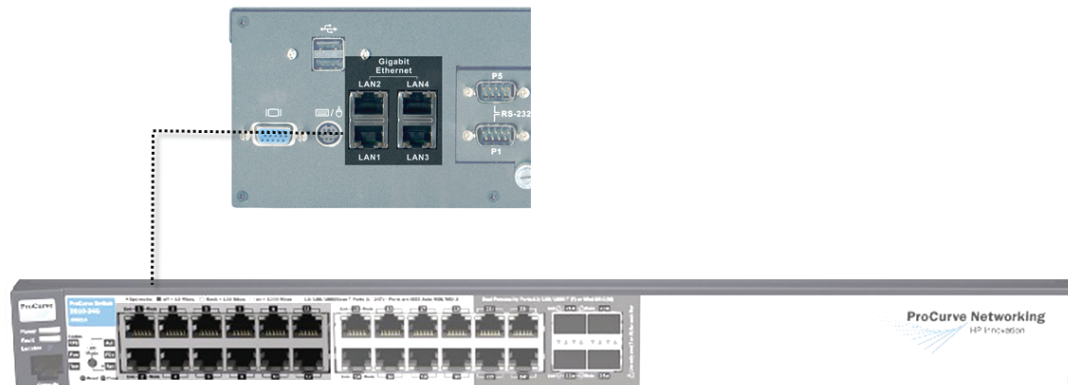
- 100 Mbps ports
- At least 16 ports
- Managed (recommended but not required)

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 MOTOTRBO Connect Plus XRT Configuration Tool.
- 4 Plug the other end into the site Ethernet switch.

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

Figure 17: XRT 9100 Gateway Connection to Ethernet Switch



4.4.2.2

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 18: LAN Cable for PC Connection



4.4.2.2.1

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 19: Null Modem Cable



4.4.3

Power Recommendations

4.4.3.1

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



4.4.3.2

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 129](#).

4.4.3.2.1

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.

4.4.4

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



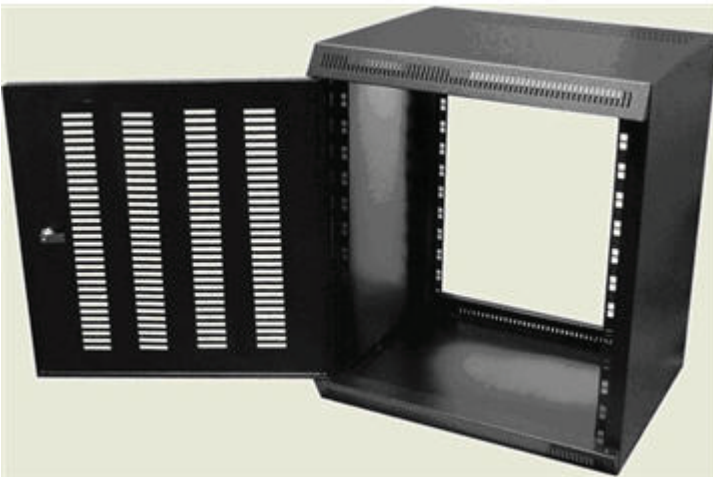
- Enclosure without a door



- 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.

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.

This page intentionally left blank.

Chapter 5

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.

5.1

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 XRT Configuration Tool to be able to communicate with the device through the Ethernet port.

When and where to use: 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 **Control Panel** → **Network and Internet** → **Network and Sharing Center**.
- 2 Click **Manage network connections**.
- 3 Select **Local Area Connection** from the list.
- 4 From the submenu, select **Change settings of this connection**.
The **Local Area Connection Properties** window appears.
- 5 Select **Internet Protocol Version 4 (TCP/IPv4)** connection and click **Properties**.
The **Internet Protocol (TCP/IP) Properties** window appears.
- 6 Select **Use the following IP address** and enter the following information:
 - IP address: 192.168.1.11 (192.168.1.10 is the default XRT IP address)
 - Subnet mask: 255.255.255.0
 - Default gateway: 192.168.1.1
- 7 Click **OK** to return to the **Local Area Connection Properties** window.
- 8 Click **OK** to complete the PC Network Communications setup.

5.2

MOTOTRBO Connect Plus XRT Configuration Tool Software

Microsoft .NET Framework Requirement: A PC can (and frequently does) have multiple versions of Microsoft .NET Framework. MOTOTRBO Connect Plus XRT Configuration Tool software for Connect Plus System Release 1.3 (or later) requires the PC to have .NET Framework version 4.0. To see what versions are on your PC, check **Control Panel** → **Add or Remove Programs**.

5.2.1

Installing MOTOTRBO Connect Plus XRT Configuration Tool Software on the PC

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

- `Setup.exe` – the application that is used to install the MOTOTRBO Connect Plus XRT Configuration Tool software on your PC
- `MOTOTRBO Connect Plus XRT Configuration Tool Setup.msi` – a 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.

5.2.2

Launching the MOTOTRBO Connect Plus XRT Configuration Tool

When and where to use:



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

Procedure:

Launch the MOTOTRBO Connect Plus XRT Configuration 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 XRT Configuration Tool application during installation.



- **Start Menu**

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

- **Program Files Folder**

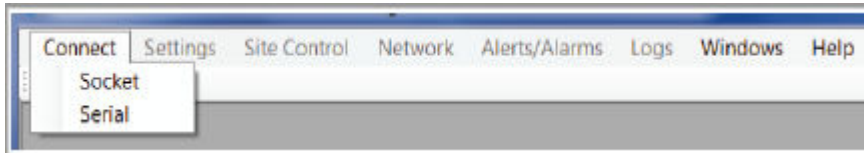
To run the MOTOTRBO Connect Plus XRT Configuration Tool Application through the `Program Files` folder, navigate to the folder, open the `Motorola Solutions` folder, locate and open the `MOTOTRBO Connect Plus XRT Configuration Tool` folder, and then double-click `MOTOTRBO Connect Plus XRT Configuration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

5.2.3 Establishing Connection with the Device

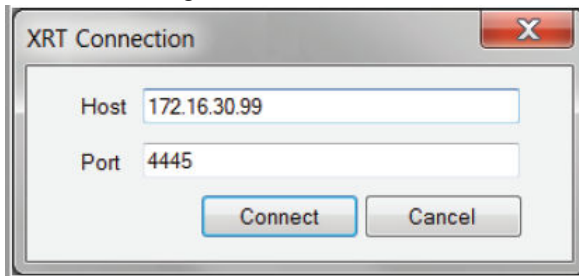
5.2.3.1 Configuring the Socket Connection

Procedure:

From the Menu Bar, select **Connect** → **Socket**.



The XRT Configuration Tool connects to XRT using port 4445.

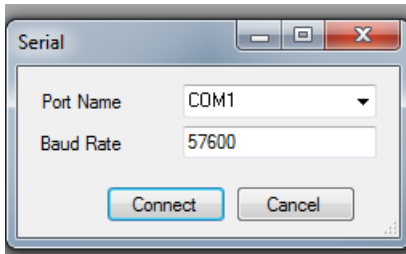


5.2.3.2 Configuring the Serial Connection

Procedure:

From the Menu Bar, select **Connect** → **Serial**

The **Serial** configuration screen appears.



The XRT Configuration Tool connects to XRT using COM1 at 57600 baud.

5.2.3.3 Logging Into the Device

Procedure:

- 1 Press the **Connect** button for either a Socket or Serial Connection.
The **Login** screen appears.



Login

Please provide your login information below

Password

Login

- 2 Enter the Password to connect to the XRT, and click **Login**.

The default password is `admin` (case sensitive), but this can be changed to a different password by using the **Change Password** screen **Site Control** → **Change Password**).

Status messages appear while the connection is being made. When the connection is complete, all of the Menu Bar options display in black text, and the words `Connected to (IP address and port)` appear in the lower left corner of the screen.

Chapter 6

Site and Network Configuration

6.1

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.

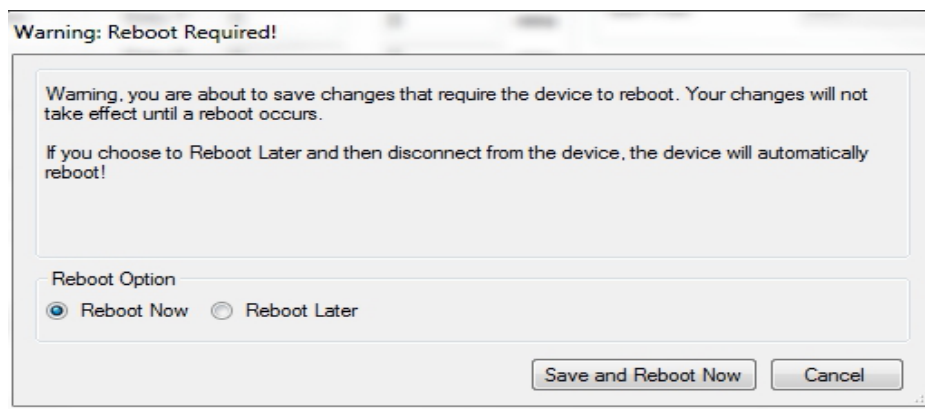
Reboot Later

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 21: Reboot Warning Prompt



6.1.1

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.

6.1.2

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.

6.1.3

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.

6.2

Configuring Network Settings

Prerequisites: Compare the Connect Plus release number of the XRT Configuration Tool software and the XRT Gateway firmware. The release number for the Configuration Tool software should be the same as (or newer than) the XRT firmware. Upgrade the XRT Configuration Tool software before proceeding any further.

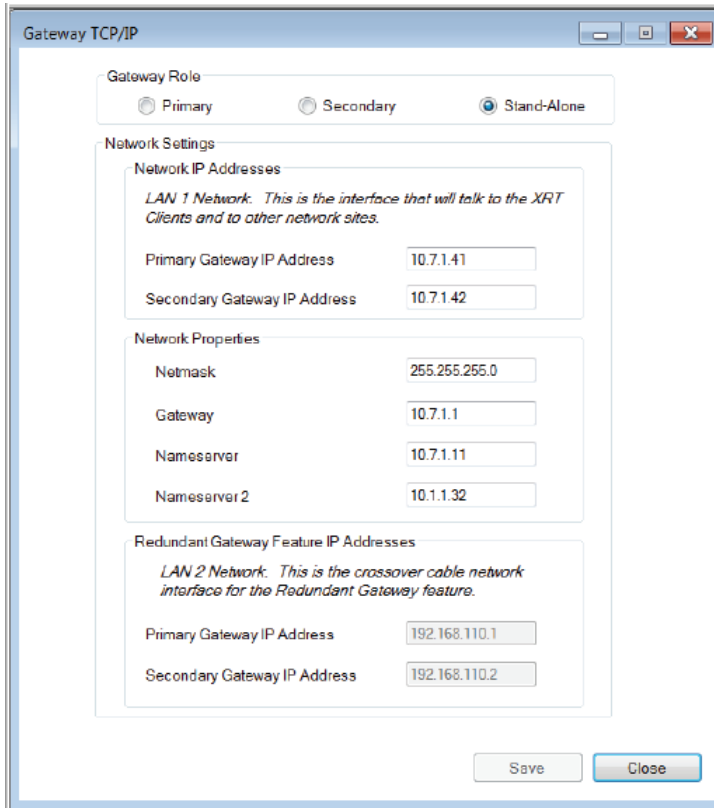
When and where to use: If the Configuration Tool software is from a prior Connect Plus Release, do not attempt to configure the XRT.

Procedure:

From the Menu Bar, select **Network** → **Settings**

The Network Configuration window appears.

Figure 22: Gateway Role and Network Settings Screen



6.2.1

Redundant XRT Gateway Capability

Beginning with Connect Plus Release 1.5, the customer can purchase a second XRT Gateway (per XRT site) to serve as backup to the primary XRT. The secondary Gateway provides backup capability, but it does not increase the number of calls that can be managed per XRT Gateway site.

The Network Configuration screen must be configured for every XRT, regardless of whether the XRT is a "stand-alone", or is part of a Redundant Gateway configuration. If the XRT site will employ a Redundant XRT Gateway configuration, read the Redundant XRT Gateway section of the MOTOTRBO Connect Plus System Planner prior to configuring this screen. 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 XRT Gateways.



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

6.2.2

XRT Gateway Role and Network Settings

The XRT Gateway can be set to one of the following roles:

Primary

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

Secondary

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

Stand-alone

Select when there is only one XRT Gateway for this XRT site (default setting).



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

6.2.2.1

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.

6.2.2.1.1

Entering the Primary IP Address

Procedure:

- 1 Enter the IP address of the primary device on its LAN 1 network.

This field is also used for the IP address of a standalone device. The format and range for the address are <000-255>. <000-255>. <000-255>. <000-255>.

- 2 Enter the primary (or standalone) 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**).

6.2.2.1.2

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.

6.2.2.1.3

Entering the IP Mask (Netmask)

Procedure:

Enter the XRT subnet mask assigned by your IT manager.
The format and range for the address are <000-255>. <000-255>. <000-255>. <000-255>.

6.2.2.1.4

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>.

6.2.2.1.5

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.

6.2.2.2

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.

6.2.2.2.1

Entering the Primary IP Address

Procedure:

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

The first three octets of this IP address must match the Secondary XRT Gateway (LAN 2) IP address exactly. The first three octets of this address must be different than the first three octets of Primary and Secondary XRT Gateway 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 XRT Gateway LAN 2 IP address assigned by your IT manager.

6.2.2.2.2

Entering the Secondary XRT Gateway IP Address

Procedure:

- 1 Enter the IP address of the Secondary XRT Gateway on its LAN 2 network.

The first three octets of this IP address must match the Primary XRT Gateway (LAN 2) IP address exactly. The first three octets of this address must be different than the first three octets of Primary and Secondary XRT Gateway 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 Secondary XRT Gateway LAN 2 IP address assigned by your IT manager.

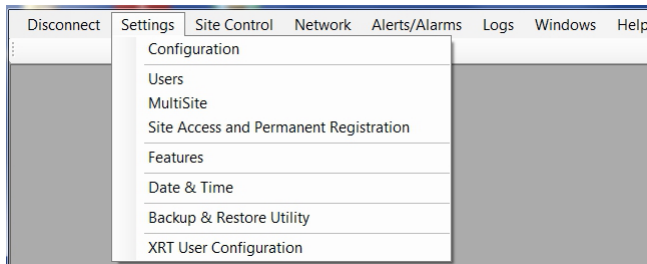
When connected to an XRT Gateway, the Status Bar at the bottom of the XRT Configuration Tool's main screen shows the current Gateway Role for the connected device; Stand-alone, Primary, or Secondary. For a Primary or Secondary Gateway, the Status Bar shows *Active* if the connected device is currently in control of Gateway operations, or *Inactive* if the connected device is not currently in control.

6.3

Configuring Site Settings

Procedure:

- 1 Select **Settings** in the Menu Bar.



- 2 Select **Configuration** in the menu.

6.3.1

Site Settings - Critical (Left Pane)



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

The following screen appears.

Figure 23: Critical Settings Configuration Screen

6.3.1.1 Site Configuration Parameters

6.3.1.1.1 Local Site ID

This is the site number of the device.

Minimum	251
Maximum	255
Increment	1
Default	255

6.3.1.1.2 Connect Plus Network ID

Connect Plus Network ID must match the Network ID programmed into all Connect Plus SUs, all XRC Controllers, and all XRT Gateways in this Connect Plus network.

Minimum	1
Maximum	4095

Increment	1
Default	1

6.3.1.2

Network Configuration Parameters

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

6.3.1.2.1

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	65335
Increment	1
Default	46000

6.3.1.2.2

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 , the XRT will listen for incoming voice packets on ports 46,000 through 46,031.

Minimum	1
Maximum	200
Increment	1
Default	32

6.3.1.2.3

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

6.3.1.2.4

Multisite Control Port

Defines the port this device will use for receiving TCP control messages from other network sites.

Minimum	4000
---------	------

Maximum	65535
Increment	1
Default	45000

6.3.1.2.5

Client TCP Port

This is the TCP port the Client Application will use to connect to the device.

Minimum	4000
Maximum	65535
Increment	1
Default	10001

6.3.1.2.6

Client UDP Start Port

This is the starting port number for the UDP ports where Client associated voice traffic will be routed to the device. The device assigns voice traffic to consecutive ports beginning with the Client UDP Start Port. The actual range of port numbers used will not be greater than the Client UDP Start Port + 1999. Although the software accepts values up to 65436, it is recommended that the configured value should not exceed 63536. Additionally, this range of ports must not overlap with the range of UDP ports defined by the two settings called **Multisite UDP Start Port** and **Max Multisite Ports**.

Minimum	1
Maximum	65436
Increment	1
Default	7700

6.3.1.2.7

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

6.3.1.3

NTP Configuration Parameters

This section describes configuration parameters for Network Time Protocol (NTP).

6.3.1.3.1

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.

6.3.1.3.1.1 **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**.

6.3.1.3.2 **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)

6.3.1.3.3 **Pool ID Configuration**

When the Client registers a Group or Multigroup talk path, the device automatically selects a Pool ID to associate with the registered Group or Multigroup. The ID is selected from the pool configured with this setting. The total number of SUIDs in the pool must be at least equal to the number of Group and Multigroup Talk Paths registered by all Clients. The recommended approach for defining the range of Pool IDs is to enter the first Pool ID in the range, followed by a hyphen, followed by the last Pool ID in the range. If the Pool IDs are not contiguous, an alternative approach is to list each Pool ID, separated by a comma. The field also accepts a combination of range expressions and comma separated entries.



IMPORTANT: Regardless of which entry method is used to express the Pool IDs (range expression or comma separated values), the Pool ID numbers must not conflict with any SUID assigned to a radio, to a Data Path ID, or to a Private Talk Path ID. See the section on Provisioning and Configuring Subscribers for additional guidance on selecting Pool ID numbers and creating user records for Pool IDs.

Each number representing an SUID must be in this range	
Minimum	1
Maximum	16776351
Field Default	blank

6.3.1.3.4 Allowing Connection From Bridge

Procedure:

Check the box labeled **Allow Bridge Connection** to permit the Capacity Max Bridge (CMB) to connect to this XRT Gateway.

When the box is checked, the XRT Gateway is dedicated to bridging calls to (and from) the Capacity Max system via the CMB. Other types of XRT Gateway Clients cannot connect to this XRT when the box is checked.

6.3.2 Site Settings - Non-Critical

The following image shows the **Site Settings — Non-Critical** configuration screen.

6.3.2.1 Call Configuration Parameters

6.3.2.1.1 Group Call Inactivity Timer (ms)

Prior to configuring the Group Call Inactivity Timer, you will need to know the Group Call Hang Time that is used by the radio network. Prior to Connect Plus Release 1.1, the Group Call Hang Time was set in the repeaters using MOTOTRBO CPS. Beginning with Connect Plus Release 1.1, the Group Call Hang Time is set in the XRC Controller using the MOTOTRBO Connect Plus Network Manager. In the XRT, set this field to be the same as the Group Call Hang Time used by the radio network.

Minimum	1000
Maximum	65535
Increment	1
Default	3000

6.3.2.1.2 Private Call Inactivity Timer (ms)

Prior to configuring the Private Call Inactivity Timer, you will need to know the Private Call Hang Time that is used by the radio network. Prior to Connect Plus Release 1.1, the Private Call Hang Time was set in the repeaters using MOTOTRBO CPS. Beginning with Connect Plus Release 1.1, the Private

Call Hang Time is set in the XRC Controller using the MOTOTRBO Connect Plus Network Manager. In the XRT, set this field to be the same as the Private Call Hang Time used by the radio network.

Minimum	1000
Maximum	65535
Increment	1
Default	5000

6.3.2.1.3

Emergency Call Inactivity Timer (s)

Prior to configuring the Emergency Call Inactivity Timer, you will need to know the Emergency Call Hang Time that is used by the radio network. Prior to Connect Plus Release 1.1, the Emergency Call Hang Time was set in the repeaters using MOTOTRBO CPS. Beginning with Connect Plus Release 1.1, the Emergency Call Hang Time is set in the XRC Controller using the MOTOTRBO Connect Plus Network Manager. In the XRT, set this field to be the same as the Emergency Call Hang Time used by the radio network.

Minimum	1 second
Maximum	601 seconds
Increment	1 second
Default	4 seconds

6.3.2.1.4

Queue Call Timeout (ms)

If the Client starts a call, but there are no repeater resources available in the Connect Plus network, the Call will be placed in the Busy Queue. This field defines the amount of time that the XRT will hold a call in the Queued state. If this time is reached without a repeater timeslot becoming available the call will be dropped.

Minimum	5000
Maximum	30000
Increment	1
Default	30000

6.3.2.1.5

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

6.3.2.1.6

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

6.3.2.1.7

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

6.3.2.1.8

Airtime Client Access: Streaming Data

When this bullet is selected, the XRT permits clients to access streaming airtime data (by sending properly formatted messages to XRT). When this bullet is not selected, the XRT does not allow clients to access to streaming airtime data.

This setting applies to all clients. To enable a specific client (also known as “user”) to access streaming data, **Billing Enabled** must be checked on the client’s user record on the **XRT User Configuration** Screen (**Settings** → **XRT User**).

6.4

Configuring for Multisite (Multisite Networks Only)

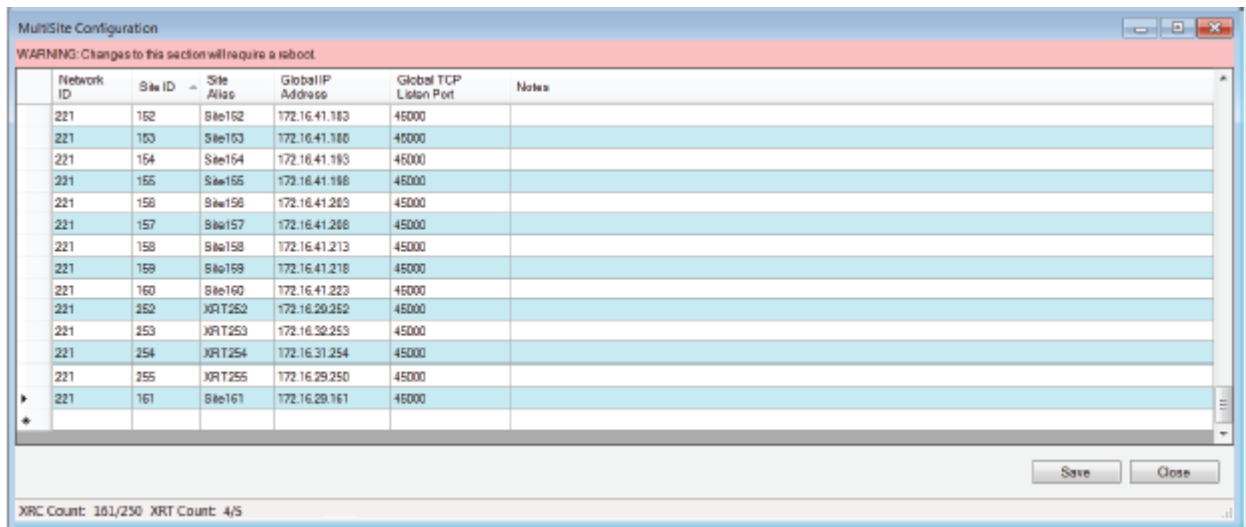
Procedure:

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

The **Multisite Configuration** window appears.

6.4.1 Multisite Settings

Figure 24: Multisite Configuration Window



The screenshot shows a window titled "MultiSite Configuration" with a warning message: "WARNING: Changes to this section will require a reboot." Below the warning is a table with the following columns: Network ID, Site ID, Site Alias, Global IP Address, Global TCP Listen Port, and Notes. The table contains 15 rows of data. At the bottom of the window, there are "Save" and "Close" buttons, and a status bar showing "XRC Count: 161/250 XRT Count: 4/5".

Network ID	Site ID	Site Alias	Global IP Address	Global TCP Listen Port	Notes
221	152	Site152	172.16.41.153	45000	
221	153	Site153	172.16.41.154	45000	
221	154	Site154	172.16.41.155	45000	
221	155	Site155	172.16.41.156	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	172.16.29.255	45000	
221	161	Site161	172.16.29.161	45000	

This screen tells XRT which other sites exist in the multisite network, and how to communicate with other network sites. The Local Site ID for the device to which you are connected should not be listed on this table. All other network sites that are currently attached (or ready to attach) to the network should be listed. This includes RF sites as well as other XRT Gateways.

6.4.1.1 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**

6.4.1.2 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**.

6.4.1.3

Connect Plus Network ID

Connect Plus Network ID must be the same network-wide. It must match the Network ID programmed into all Connect Plus XRC Controllers and radios.

Minimum	1
Maximum	4095
Increment	1
Default	Network ID in Settings → Configuration → Site Network ID

6.4.1.4

Site ID

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

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

6.4.1.5

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.

6.4.1.6

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)>.

6.4.1.7

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

6.4.1.8

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 7

System Management

7.1

Provisioning and Configuring XRT Subscribers

7.1.1

Initial XRT Integration in the Connect Plus Network

After successfully installing the XRT and configuring it with an IP address and its multisite neighbors, the XRT will require subscriber provisioning. If the XRT is being added to an existing network (that already has subscriber records defined), use the MOTOTRBO Connect Plus Network Manager User Health Tool to copy the user database (also called the user registry) from a site with an up-to-date user database to the XRT Gateway. This will populate the XRT user database with the user records copied from the other site. Subsequent edits to the user database, no matter where they occur in the network, will be automatically shared between all network sites, including the XRT.

The User Health Tool, which was introduced in Connect Plus System Release 1.4, requires a network connection between the source and target sites. For more information, see [User Health Tool on page 98](#).

Three types of records are contained in the user database:

- 1 **User Records** (also called Unit IDs and SUIDs): A User Record always points to single entity. The entity can be any of the following:
 - a A Connect Plus portable or mobile radio: User Records for Connect Plus radios are shown in XRT user database, but they are typically managed (edited) from a Connect Plus XRC controller, not from the XRT. Do not edit user records for Connect Plus radios unless this is an accepted and approved strategy for managing radios on the network.
 - b A Private Talk Path ID registered by a XRT Client: This type of user record allows the XRT Client to participate in individual call types (Private Call, for example), much like a Connect Plus radio. User records for Private Talk Path IDs are typically configured into the XRT (and then automatically propagated network-wide). Do not use IDs that have already been assigned to a Connect Plus radio, or that have been assigned as a Pool ID.
 - c A Data Path ID registered by a XRT Client: This type of user record allows the XRT Client to initiate and receive packet data calls. User records for Data Path IDs are typically configured into the XRT (and then automatically propagated network-wide). Do not use IDs that have already been assigned to a Connect Plus radio, that have been assigned as a Private Talk Path ID, or that have been assigned as a Pool ID. On the user record that corresponds to a Data Path ID, check the box labeled **Packet Data Call Enabled**.
 - d A Pool ID: When the Client registers a Group or Multigroup talk path, the XRT automatically selects a Pool ID to associate with the registered Group or Multigroup. Defining and creating Pool IDs is a two-step process:
 - a Define which numbers will be used as Pool IDs in the Pool ID field (**Settings** → **Configuration**). The total number of IDs in the pool must be at least equal to the number of registered Group and Multigroup talk paths. Do not use IDs that have already been assigned to a Connect Plus radio, that have been assigned as a Private Talk Path ID, that have been assigned as a Data Path ID, or that have been configured as Pool IDs at any other XRT site in the same network. Using numbers in the sixteen million range for Pool IDs (for example, 16,000,001 through 16,000,100) usually avoids conflicts with Connect Plus radios. To be

certain, check the user database prior to defining the Pool ID range or creating user records for Pool IDs.

- b The second step in defining/creating Pool IDs, is to create a user record (**Settings** → **Users**) for each ID that was defined in the Pool ID field. User records for Pool IDs are typically configured into the XRT (and then automatically propagated throughout the network). Do not use IDs that have already been assigned to a Connect Plus radio, that have been assigned as a Private Talk Path ID, or that have been configured as Pool IDs at any other XRT site in the same network.

2 Group Records: This is a shared ID that allows conversation between two or more radios that are programmed with the same Group ID. When registered by the XRT Client, it is referred to as a Group Talk Path, but the registration points to the same Group record that is used by the radios. This is what allows the Client to initiate calls to radios in the group, and to receive calls from radios in the group.

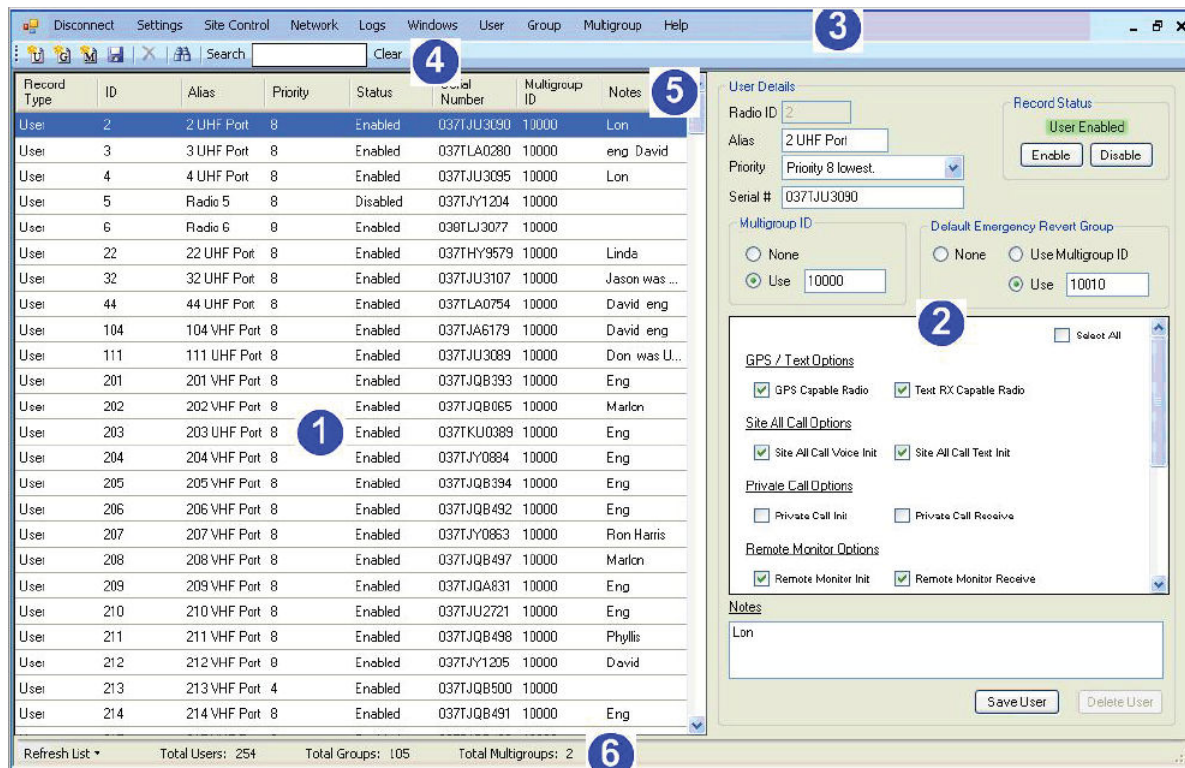
3 Multigroup Records: This is a special type of shared ID that provides the ability to make an announcement to all radios that have been configured with the same Multigroup ID. If the Multigroup Call is initiated by the XRT Client, radios are not allowed to talk back during the Call Hang Time. If the Multigroup Call is initiated by a radio, other radios are not allowed to talk back during the Call Hang Time, but the XRT Client is allowed to talk back. When the ID is registered by the XRT Client, it is referred to as a Multigroup Talk Path, but the registration points to the same Multigroup record that is used by the radios.

IDs used during Client voice transmissions: When the XRT Client transmits during a Group or Multigroup Call, it sends two IDs in the voice transmission. **The Destination ID** is set to be the same as the Group or Multigroup Talk Path that is being used for the call. The Destination ID is validated by the Connect Plus network, so there must be a record in the user database for the Destination ID. The Client also sets the Source ID for the voice transmission. The **Source ID** in the Client's voice transmission is not currently validated by the Connect Plus network, but it is passed through to the receiving radios, where it is shown on the radio's display as the "PTT-ID". Even though Connect Plus is not currently validating the Source ID in the Client's voice transmission, there are two very important recommendations about the Source ID used by the Client:

- If at all possible, the Client should use a registered Private Talk Path ID as the Source ID in the Group/Multigroup voice transmission. This has several advantages:
 - Because there must be a user record in the subscriber database for a Private Talk Path ID, the ID is not likely to conflict with a radio.
 - This ID can then be configured into the Call List for the receiving radios so that the alias identifies the individual (or console position) making the transmission.
 - The radio user can then use this same number to make a Private Call back to the Client, if so desired.
- If the recommendation above cannot be followed for some reason, at the very least the Client should make sure that the Source ID used in its voice transmission does not conflict with any assigned Radio ID. If it does, the radio user will likely think that the transmission is coming from another radio, not from the XRT Client. The best way to assure that the ID does not conflict with a Radio ID is to create a user record for the Source ID in the user database. The record then serves as a placeholder so that the ID will not be assigned to a Connect Plus radio.

7.1.1.1 User Registry Window

Figure 25: User Registry Window



The following list explains each field labeled within the **User Registry** window.

1. Display Area

Shows a list of one or more user records.

2. Details Area

Shows the details of the user record that is currently selected in the Display Area.

3. Menu Bar

Contains buttons for Users, Groups, and Multigroups.

4. Submenu Bar

Contains controls for adding new records, deleting records, and sorting records.

5. Header (Sort)

Can sort the records in ascending or descending order by the selected field. Click on a header to sort ascending, click again for descending.

6. Display Area Totals

Details the total number of Users, Groups, and Multigroups in the list. Also, this area contains a Refresh List button that pulls the most current user records from XRT.

7.1.1.1.1

Launching the User Registry Window

Procedure:

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

The **User Registration** window appears.

7.1.2 User Details

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

Figure 26: User Details Screen

7.1.2.1 Radio ID

This field contains the subscriber ID (SUID) of the radio, Private Talk Path ID, Data Path ID, or Pool ID corresponding to this record.

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



NOTICE: If a Radio ID number is entered that does not conform to the expected Radio ID number format, an exclamation point (!) 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 Radio ID number.

7.1.2.2

Alias

This field contains the alphanumeric alias for the Subscriber Unit corresponding to this record (optional). The alias can be used to identify user records that have been created for Client Private Talk Path IDs, Data Path IDs, and/or Pool IDs.

Minimum	-
Maximum	255 characters
Increment	-
Default	Blank

7.1.2.3

Record Status

This field is used to display and change the status of the user record for this SUID.

Changing the status of a subscriber here will propagate that change to all networked XRC Controllers and will allow or disallow registration of the specified unit. If the unit is currently on but disabled, then clicking the Enable button will send the Enable Command over the air and allow the unit to register. Conversely, if the unit is on and registered on the Connect Plus network, then click the Disable button will send the Disable Command over the air deregistering the unit and disallowing reregistration.

When creating user records for Private Talk Path IDs, Data Path IDs, or Pool IDs, make sure that the Record Status is set to **User Enabled**.

7.1.2.4

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.

7.1.2.5

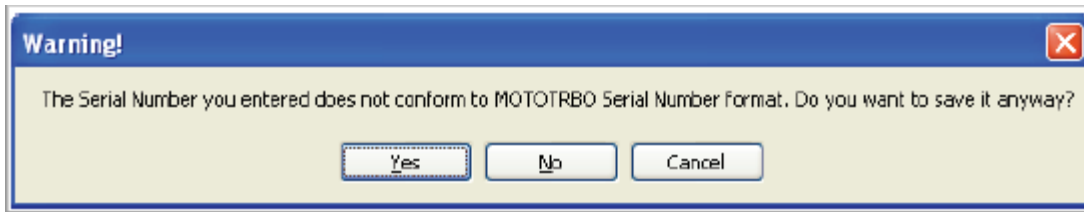
Serial Number

If this User Record is for a radio unit, enter the ten-character MOTOTRBO Serial Number for the radio corresponding to this record. It is not necessary to enter a Serial Number when creating a user record for a XRT Client Private Call Talk Path, Data Path, or a Pool ID.

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

It is not necessary to enter a Serial Number when creating a user record for a XRT Client Private Call Talk Path, Data Path, or a Pool ID. When you attempt to save a User Record with a blank Serial Number, the warning in the following figure appears.

Figure 27: Serial Number Warning



7.1.2.6

Multigroup ID

A Connect Plus radio can receive transmissions on its Multigroup ID, even when the radio is selected to a different Group. To enter a Multigroup ID for a Connect Plus 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. Select the bullet labeled None if the radio corresponding to this record does not use a Multigroup ID, or when creating a user record for a Private Talk Path ID, Data Path ID, or Pool ID used by XRT Clients. User records for Pool IDs are a special case because the XRT can automatically select the **Use** bullet and write a Multigroup ID number into this field, if and when needed.

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.

7.1.2.7

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 74](#).
- **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 75](#) and [Entering the Physical Serial Number on page 75](#).



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.

7.1.2.7.1

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](#)

7.1.2.7.2

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.

7.1.2.7.3

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.

7.1.2.7.4

Saving of Records Containing a Physical Serial Number

When the XRT Configuration Tool (or 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 Connect Plus database. If there is a conflict in any key portion of the Physical Serial Number, the software 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 software 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 there is not 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 labeled **Enable Physical Serial Number Authentication**. You must obtain a valid, non-conflicting, Physical Serial Number prior to enabling Physical Serial Authentication for this user.

7.1.2.8

Default Emergency Revert Group

Configure Default Emergency Revert Group as follows: If the user record corresponds to an XRT Client Private Talk Path, Data Path ID, or Pool ID, select the bullet labeled **None** (the default setting). If the user record corresponds to a Connect Plus subscriber radio, this setting indicates which Talk Group ID the SU will use when initiating or receiving an Emergency Call or Emergency Alert on its Default Emergency Revert Group ID. The information entered here must match subscriber radio programming with Connect Plus CPS.

7.1.3

User Details Check Boxes

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

- **GPS Capable Radio**
- **Indoor Location Reporting Capable**
- **Text RX Capable Radio**
- **Site All Call Text Init**
- **Private Phone Call Init**
- **Private Phone Call Receive**

- **Exclude from CIRC**

When creating user records for Client Private Talk Path IDs, Data Path ID, and Client Pool IDs, it is recommended to check the boxes listed below. Other boxes can be left unchecked. (Not all of the boxes listed below apply to both Private Talk ID and Pool ID records, but there is no harm in configuring both types of records the same for these check boxes).

Figure 28: 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 Confirmed Transmission

Generic Data Call Enabled

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

7.1.3.1

Site All Call Voice Init

The XRT automatically checks this box if the user record corresponds to a Pool ID that the XRT has selected to register with the Network Wide All Call (NWAC) Talk Path. NWAC uses the same Group ID that a radio uses to initiate a Site All Call. If a radio-initiated Site All Call is currently in progress at a site when the XRT Client initiates a NWAC, the NWAC will not be heard at that site (and it will not be placed in the Busy Queue). To prevent this potential conflict, the Network Administrator may wish to uncheck this box on all user records that correspond to subscriber radios.

7.1.3.2

Authorizing Private Call Init

Procedure:

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

7.1.3.3

Authorizing Private Call Receive

Procedure:

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

7.1.3.4

Enabling Packet Data Call

Procedure:

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

7.1.3.5

Enabling Generic Data Call

Procedure:

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

7.1.3.6

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.

7.1.3.7

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.

7.1.3.8

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.

7.1.3.9

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.

7.1.3.10

Authorizing Disable Command Receive

Procedure:

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

7.1.3.11

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).

7.1.3.12

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.

7.1.3.13

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.

7.1.3.14

Authorizing Radio Check Init

Procedure:

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

7.1.3.15

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.

7.1.3.16

Authorizing Emergency Init

Procedure:

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

7.1.3.17

Notes

An alphanumeric string can be used to create a note about the SU corresponding to this entry (optional). 225 maximum character limit. The Notes field can be used to clearly identify user records that have been created for Client Private Talk Path IDs, Data Path IDs, and/or Pool IDs.

7.1.4

Group Details Screen

Figure 29: Group Details Screen

The screenshot shows a web-based form titled "Group Details". On the left, there are several input fields: "Group ID" with the value "1001", "Alias" (empty), "Priority" with a dropdown menu showing "Priority 8 lowest configurable priority.", "Allow Phone Access" with an unchecked checkbox, and "Enable Priority Monitor" with an unchecked checkbox. Below these is a large empty text area. On the right, there is a "Record Status" section with a green box containing "Group Enabled" and two buttons: "Enable" and "Disable". At the bottom of the form are two buttons: "Save Group" and "Delete Group".

7.1.4.1

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.

7.1.4.2

Alias

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

7.1.4.3

Record Status

This field is used to display and change the status of the user record for this SUID.

Changing the status of a subscriber here will propagate that change to all networked XRC Controllers and will allow or disallow registration of the specified unit. If the unit is currently on but disabled, then clicking the Enable button will send the Enable Command over the air and allow the unit to register. Conversely, if the unit is on and registered on the Connect Plus network, then click the Disable button will send the Disable Command over the air deregistering the unit and disallowing reregistration.

When creating user records for Private Talk Path IDs, Data Path IDs, or Pool IDs, make sure that the Record Status is set to **User Enabled**.

7.1.4.4

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.

7.1.4.5

Allowing Phone Access

Procedure:

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

7.1.4.6

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 it 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.

7.1.4.7

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.

7.1.5

Multigroup Details

Figure 30: Multigroup Details Screen

Multigroup Details

Multigroup ID: 10000

Alias: [Text Field]

Priority: Priority 2 highest configurable priority

Allow Phone Access:

Enable Priority Monitor:

Record Status: Multigroup Enabled

Buttons: Enable, Disable, Save Multigroup, Delete Multigroup

7.1.5.1

Multigroup ID

A Connect Plus radio can receive transmissions on its Multigroup ID, even when the radio is selected to a different Group. To enter a Multigroup ID for a Connect Plus 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. Select the bullet labeled None if the radio corresponding to this record does not use a Multigroup ID, or when creating a user record for a Private Talk Path ID, Data Path ID, or Pool ID used by XRT Clients. User records for Pool IDs are a special case because the XRT can automatically select the **Use** bullet and write a Multigroup ID number into this field, if and when needed.

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.

7.1.5.2

Alias

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

7.1.5.3

Record Status

This field is used to display and change the status of the user record for this SUID.

Changing the status of a subscriber here will propagate that change to all networked XRC Controllers and will allow or disallow registration of the specified unit. If the unit is currently on but disabled, then clicking the Enable button will send the Enable Command over the air and allow the unit to register. Conversely, if the unit is on and registered on the Connect Plus network, then click the Disable button will send the Disable Command over the air deregistering the unit and disallowing reregistration.

When creating user records for Private Talk Path IDs, Data Path IDs, or Pool IDs, make sure that the Record Status is set to **User Enabled**.

7.1.5.4

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.

7.1.5.5

Allowing Phone Access

Procedure:

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

7.1.5.6

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 it 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.

7.1.5.7

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.

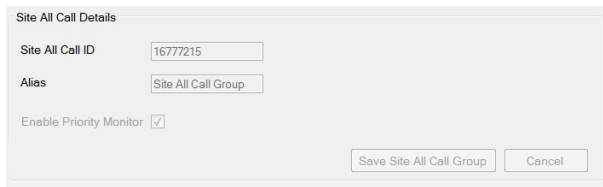


NOTICE: This field is optional.

7.1.6

Site All Call Details

Figure 31: Site All Call Details Screen



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.

7.1.6.1

Enabling Priority Monitor

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

7.1.7

Creating Subscriber/Group/Multigroup Records

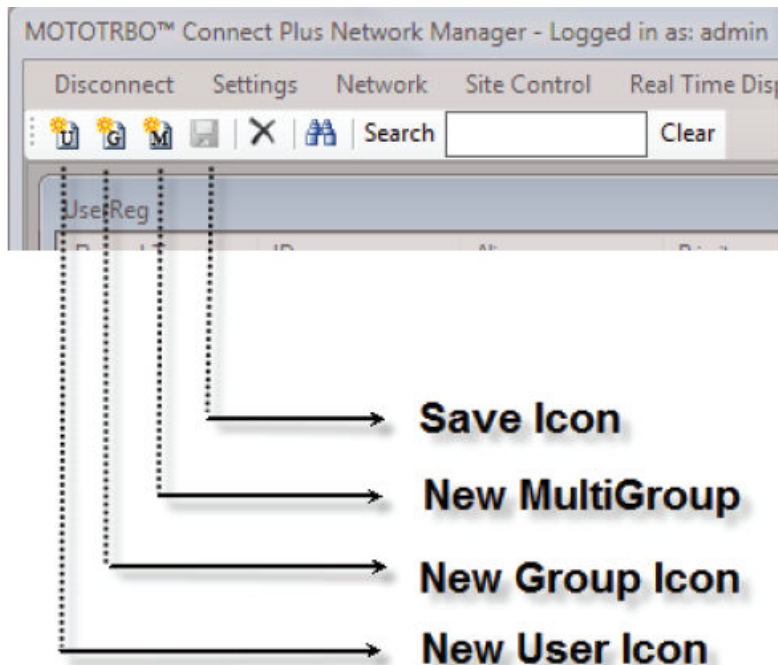
The following sections describe ways of creating records using the **Menu Bar** → **Submenu Bar** → **Display Field**.

7.1.7.1

Submenu Bar for Records Creation

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

Figure 32: Icons Within the Submenu Bar



7.1.7.1.1

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.

7.1.7.1.2

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**.

7.1.7.1.3

Creating a New Group

Procedure:

- 1 From the Menu Bar, select **Settings** → **Users**.
- 2 Right-click within the **Group** display field and select **New** from the menu.
The **Group Details** on the right side of the screen are cleared.
- 3 Enter the Group information.
- 4 Click **Save** on the submenu bar or **Save Group** at the bottom of the **Group Details** box to save the record.

7.1.7.1.4

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.

7.1.7.1.5

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.

7.1.8

Locating Subscriber/Group/Multigroup Records

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

7.1.8.1

Using the Submenu Bar Find Tools

The following image displays the User, Group and Multigroup options under the Menu Bar.

The screenshot shows a software interface with a menu bar (Disconnect, Settings, Site Control, Network, Logs, Windows, User, Group, Multigroup, Help) and a submenu bar (Search, Clear). Below the submenu bar is a table with columns: Record Type, ID, Alias, Priority, Status, Serial Number, Multigroup ID, and Notes. The table contains 10 rows of user records. Below the table are summary statistics: Refresh List, Total Users: 59931, Total Groups: 15996, Total Multigroups: 3. A 'UserReg' button is visible. At the bottom, it says 'Connected to 172.16.29.179 on Port 4445' and 'Site Number: 254'. A search dialog box titled 'Enter ID / Alias to find' is shown, with a text input field and 'Find' and 'Cancel' buttons. Three callout lines point to the search icon, the search text box, and the dialog box.

Record Type	ID	Alias	Priority	Status	Serial Number	Multigroup ID	Notes
User	1		8	Disabled	038TLW5064	10000	
User	2	2 UHF Port	3	Disabled	0377JU3090	10000	
User	3	3 UHF Port	7	Disabled	037TLA0742	10000	
User	4	USER #4	2	Disabled	037TLUB092	10000	TEST U
User	5	1234567890123456...	8	Enabled	0377JY1204	10000	
User	6		8	Enabled	038TLW3582	10000	
User	7		8	Enabled	037TLW6490	10000	
User	8		8	Enabled	038TMC6422	10000	
User	9		8	Disabled	038TLW5064	10000	
User	10	10 800/900 Port	8	Enabled	777TLG0804	10000	

7.1.8.1.1

Searching Records Using the Find Icon

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 From the Menu Bar, select **Settings** → **Users**.
- 2 Click the **Find** icon on the submenu bar.

The **Enter ID / Alias** dialog box appears.

- 3 Enter a search string consisting of letters and/or numbers and click **Find**.

The screen displays all records that match the search criteria in the ID, Alias, Status, Serial Number, Multigroup ID or Notes fields.

7.1.8.1.2

Searching Records via the Text Box

Procedure:

- 1 From the Menu Bar, select **Settings** → **Users**.
- 2 Click inside the **Search Text Box** on the submenu bar.
- 3 Enter a search string consisting of letters and/or numbers.



NOTICE: In order to reduce the number of possible matches, type as much information about the desired record as possible.

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.

7.1.9

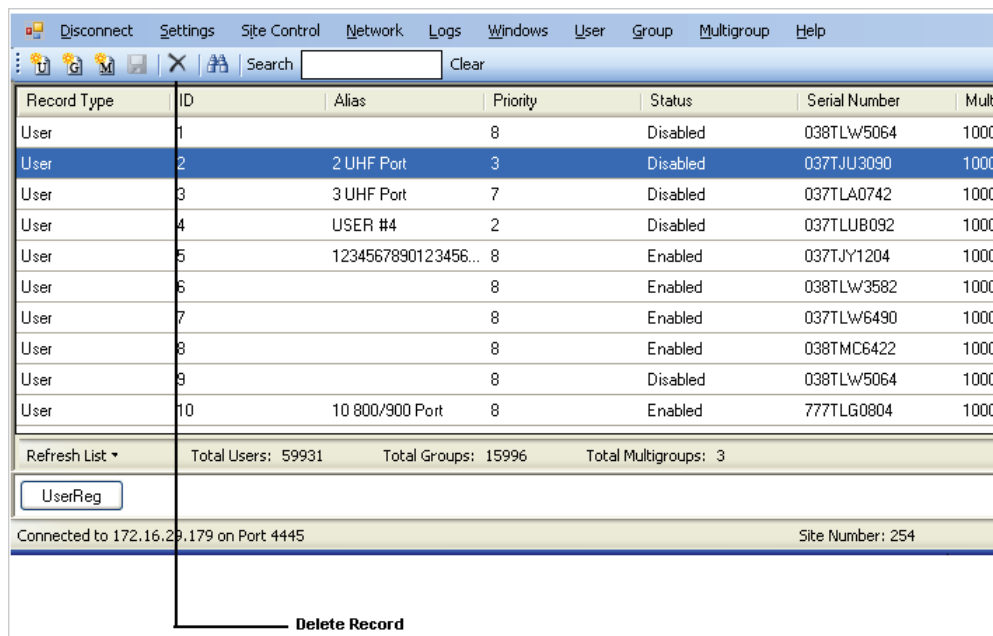
Deleting Subscriber/Group/Multigroup Records

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

7.1.9.1

Submenu Bar for Deleting Records

The following image shows the **Delete Record** icon in the Submenu Bar.



7.1.9.1.1

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.

7.1.9.1.2

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.

7.1.9.1.3

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.

7.2

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.

7.2.1

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.

7.2.2

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.

7.2.3

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

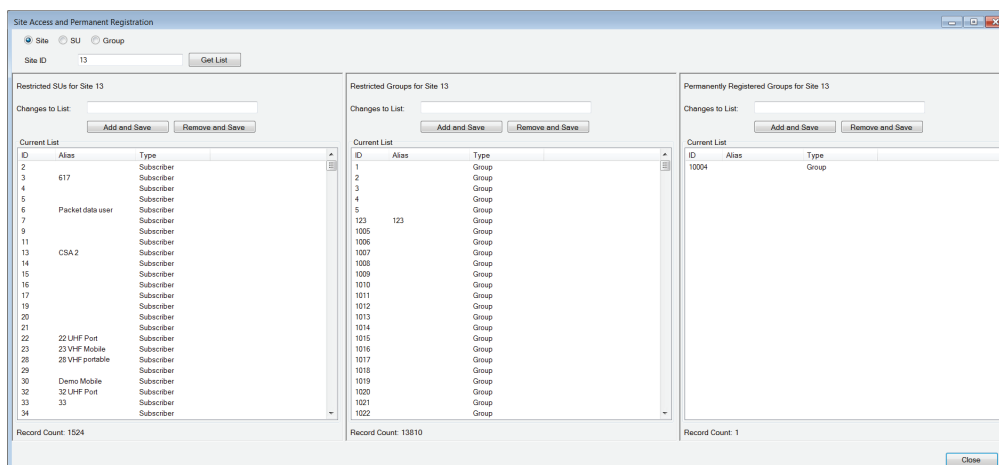
Procedure:

- 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 $\langle n \rangle$ =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.



- 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 90](#).

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.

7.2.4

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 $\langle n \rangle$ =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.

7.2.5

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 $\langle n \rangle$ =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.

7.2.6

Configuring a List of Restricted Sites for a Specific Radio

Procedure:

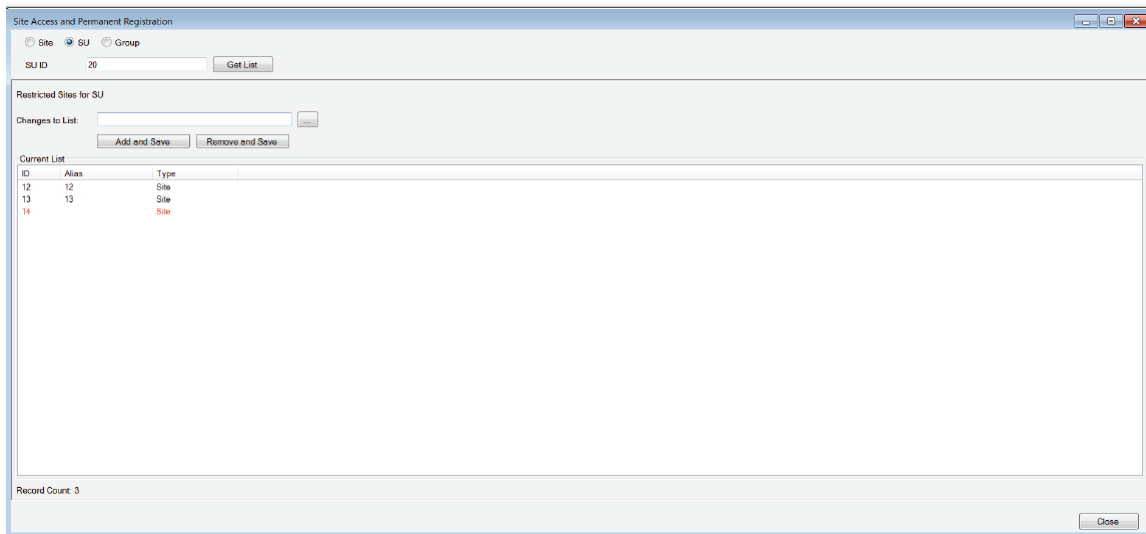
- 1** Launch the **Site Access and Permanent Registration** screen.
- 2** Click **SU** bullet (if not already selected).
- 3** Enter the SUID to be configured into the **SU ID** field.

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 33: Current List



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 90](#).
- 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.

7.2.7

Configuring a List of Restricted Sites for a Specific Talk Group ID

Procedure:

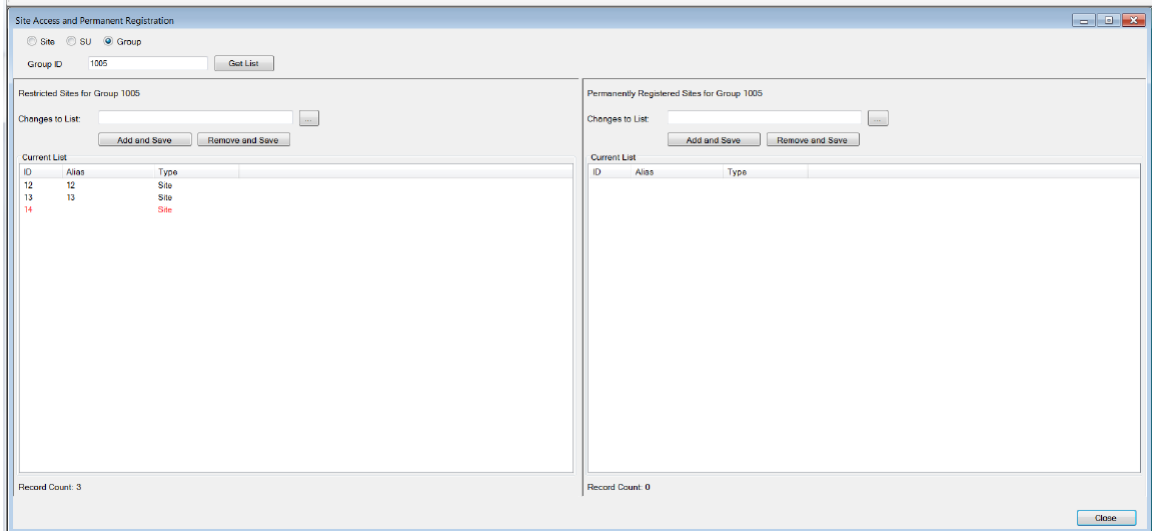
- 1** Launch the **Site Access and Permanent Registration** screen.
- 2** Click on **Group** bullet (if not already selected).

- 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.



- 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 90](#).
- 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.

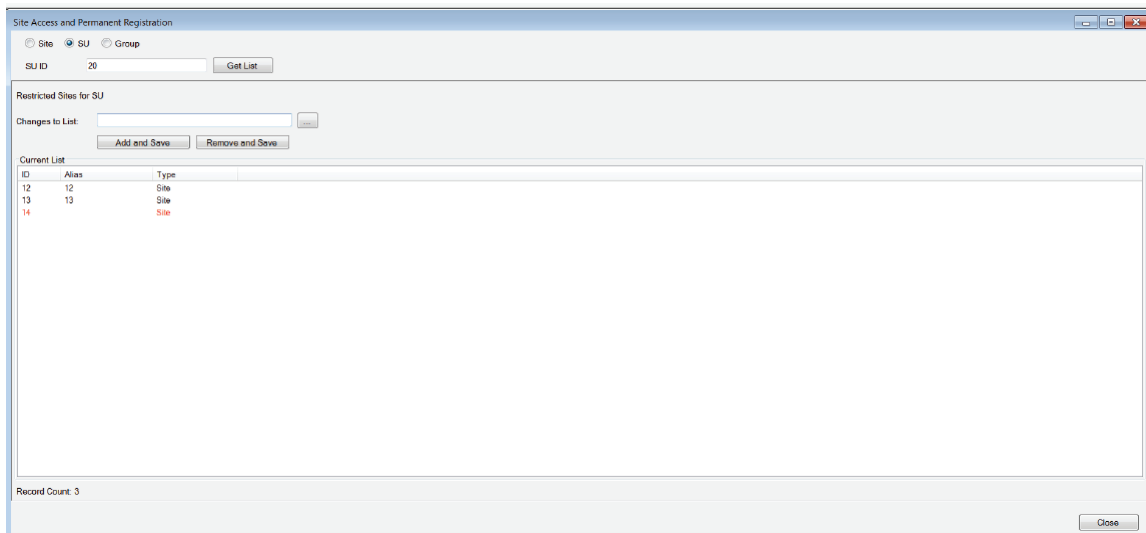
7.2.8


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.



- 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 90](#).
 - 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.

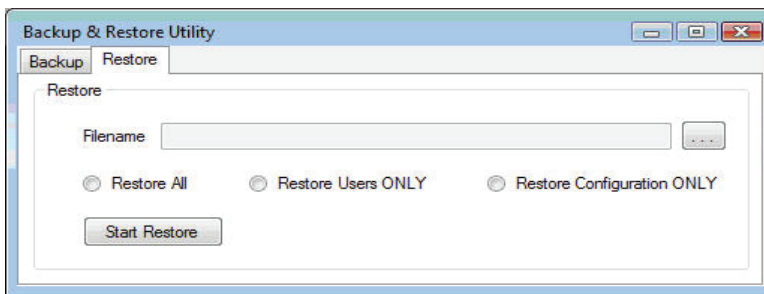
The system checks and validates the submitted changes. After validating the changes, the application updates the Current List if all changes are accepted, or responds with an appropriate error indication for the first rejected change (due to the validation check). Normally all changes must be accepted 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.

7.3

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 34: 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.

7.3.1

Saving a Site Configuration and User Records to a File

Procedure:

- 1 From the Menu Bar, select **Settings** → **Backup & Restore Utility**.
The **Backup & Restore Utility** window appears.
- 2 On the **Backup** tab, click the browse (...) icon, select the location to save the site configuration, and click **Save**.
- 3 Click **Start Backup**.
The message `Backup completed successfully!` appears.

7.3.2

Restoring a Site Configuration from a File

When and where to use:

Beginning with Connect Plus Release 1.4, the recommended method for restoring users is to use the MOTOTRBO Connect Plus Network Manager User Health Tool to copy the user database (also called the user registry) from a site with an up-to-date user database. This will populate the user database of the device with the user records copied from the other site. Subsequent edits to the user database, no matter where they occur in the network, will be automatically shared between all network sites. The User Health Tool requires a network connection between the source and target sites. For more information, see [User Health Tool on page 98](#).

Procedure:

- 1 From the Menu Bar, select **Settings** → **Backup & Restore Utility**.

The **Backup & Restore Utility** window appears.

- 2 On the **Restore** tab, click the browse (...) icon, select the file to be restored, and click **Open**.

- 3 Click a bullet to show which parts of the backup information should be uploaded.

- 4 Click **Start Restore**.

A message appears, asking to confirm restoration and reboot.

- 5 Click **Yes** to restore or **No** or **Cancel** to stop the restore.

A progress bar displays the status of the restore. When the restore is complete, a message appears: `File restore completed successfully! Rebooting...`

7.3.2.1

User Health Tool

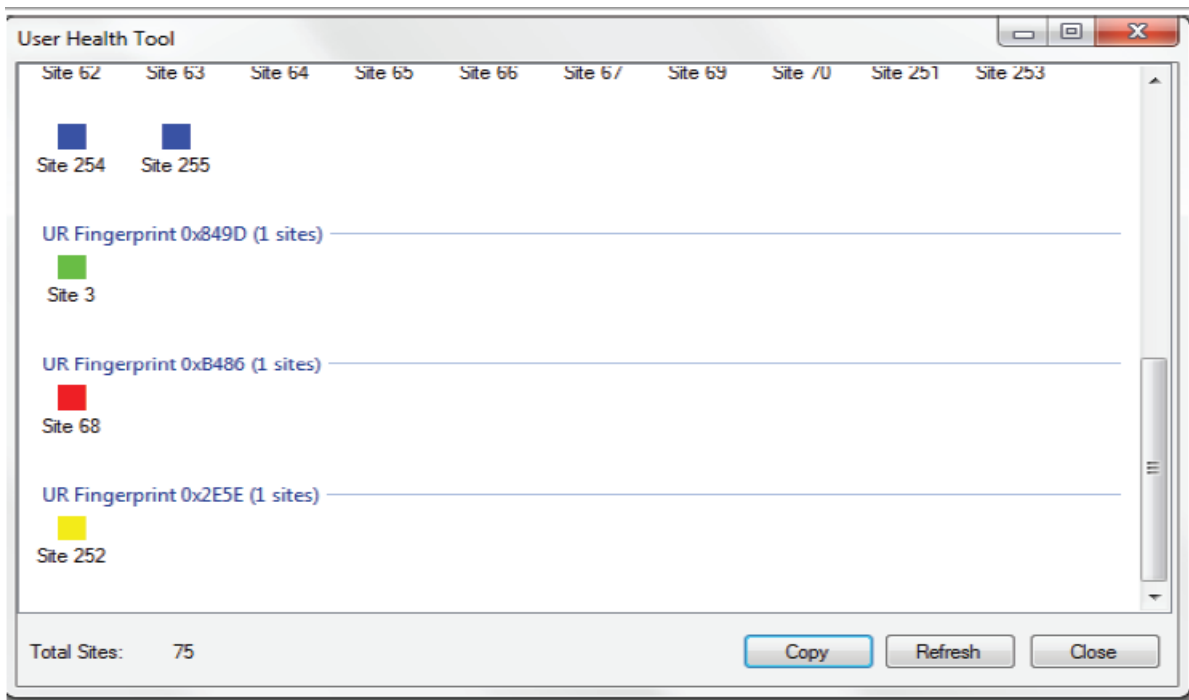
In multisite networks, it is imperative that all sites maintain an identical copy of the User Database (also called the "User Registry"). This is the database of subscriber radios, talkgroups, multigroups, pool IDs, private talkpath IDs, etc. In normal operation the sites automatically share updates 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 35: User Health Tool Screen



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.

7.4

Site Control

7.4.1

Rebooting a Site

When and where to use:

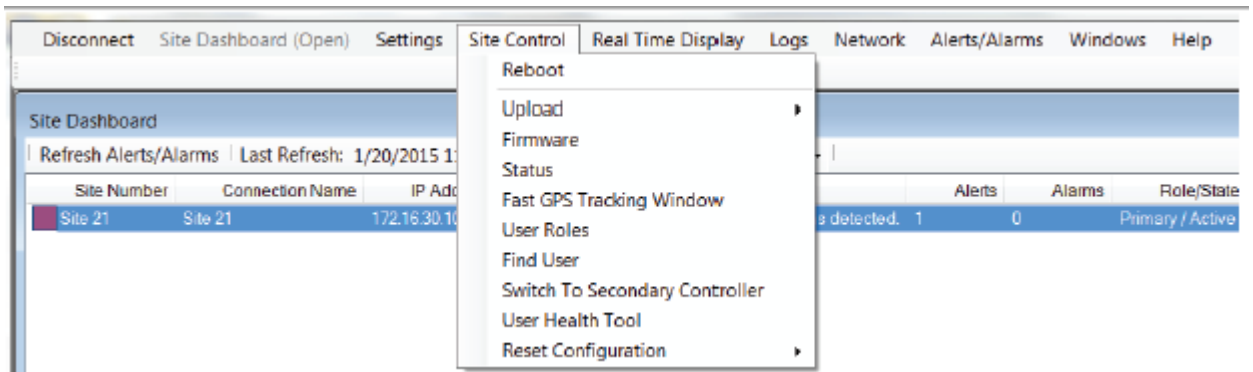


CAUTION: Rebooting an operational device has a significant impact on site operations. If a reboot must occur, it should be done at a time that will have the least possible impact on site operation (if possible). The following is a partial list of what occurs when a site reboots:

- 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.

7.4.2

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 101](#).
- 3 Run the command to upgrade to the uploaded firmware file. See [Upgrading the Firmware on page 101](#).

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.

7.4.2.1

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.

7.4.2.2

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.

7.4.2.3

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.

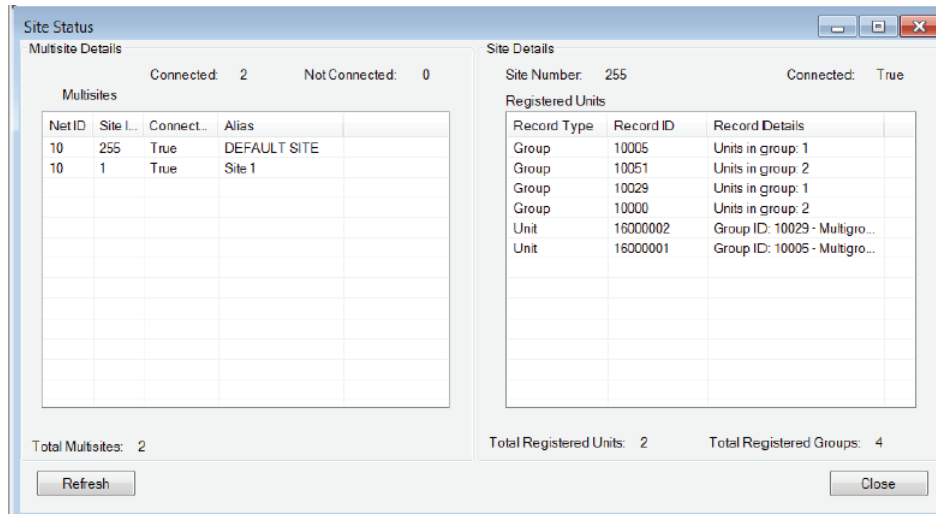
- 3 Click **Yes** to upgrade or **No** or **Cancel** to stop the upgrade.

7.4.3

Site Status Window

The **Site Status** window is divided into two parts.

Figure 36: Site Status Window



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.

7.4.3.1

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.

7.4.4

Changing a Password

Procedure:

- 1 Click on within the menu. From the Menu Bar, select **Site Control** → **Change Password**.

The **Change Password** screen appears.

The screenshot shows a 'Change Password' dialog box with a blue title bar. Inside, there are three text input fields: 'Old Password' with five dots, 'New Password' with seven dots, and 'Confirm Password' with seven dots. Below the fields are two buttons: 'Save Changes' and 'Cancel'.

- 2 If the **Old Password** field appears, then enter the old password.
- 3 In the **New Password** field, enter the new password that will be used (beginning with the next connection).

The new password must contain between 5 and 30 characters. Alpha characters (a-z) are case sensitive. Numbers, special characters, and spaces are allowed (a space counts as a character).
- 4 In the **Confirm Password** field, re-enter the new password as confirmation.
- 5 Click **Save Changes**.

7.4.5

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 Gateway**.
- When connected to the Secondary device, and the Secondary device currently has control, the menu item says **Switch to Primary Gateway**.
- 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.



NOTICE: 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.

7.4.6

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.

7.5

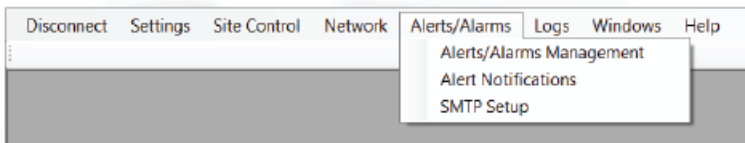
Alerts and Alarms Management

7.5.1

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 37: 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.

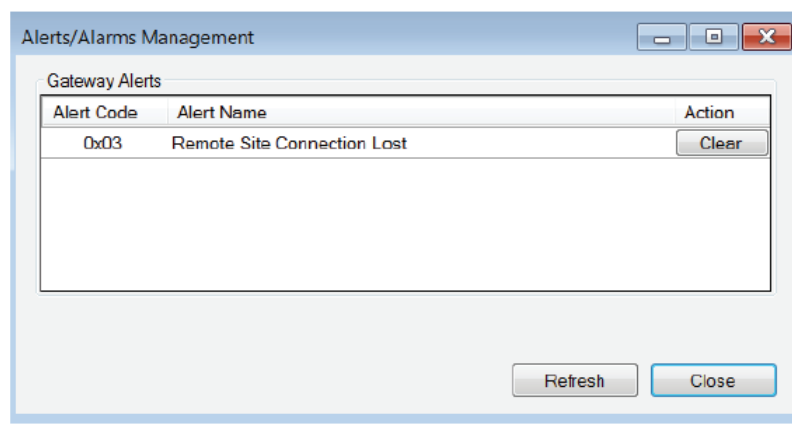
7.5.2

Launching the Alerts/Alarms Management Window

Procedure:

From the Menu Bar, select **Alerts/Alarms** → **Alerts/Alarms Management**

The **Alerts/Alarms Management** window appears. The window shows any active XRT Gateway Alerts.



7.5.2.1


XRT Gateway Alerts

An XRT Gateway Alert is raised when an underlying fault condition occurs.

Once a Gateway Alert is raised, the alert stays active until it is manually cleared by the XRT Configuration Tool user. This operation has several implications for the XRT Configuration Tool user:

- The underlying fault that triggered the Gateway Alert may or may not be still present. It is the responsibility of the technician to investigate further.
- Once the technician has confirmed that the underlying fault is no longer present, he/she must manually clear the Gateway Alert.
- If the underlying fault condition is still present when the technician clears the Gateway Alert, the XRT will raise the Gateway Alert again. This bears further investigation.

Alert Message	Description
Remote Site Connection Lost	Occurs if a remote site has lost connection for more than 1 minute.

Secondary Gateway Active	This alert is shown by the Secondary Gateway, after it takes over site control from the Primary Gateway.
Primary Gateway missing connected Secondary Gateway	Indicates that the Primary Gateway has yet to communicate with the Secondary Gateway, or that communication has been established, but the process of synching with the Secondary Gateway is not yet complete.
System Health Alert	This alert is raised upon detection of certain conditions that may be detrimental to hardware or software performance. When the alert is raised, an Event Log entry is also created. The Event Log entry contains a "System Health issue number" that can be provided to Motorola Solutions technical support personnel for further investigation.
NTP Server Conflict	<p>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</p> <p> 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.</p>

7.5.2.2

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.

7.5.3

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

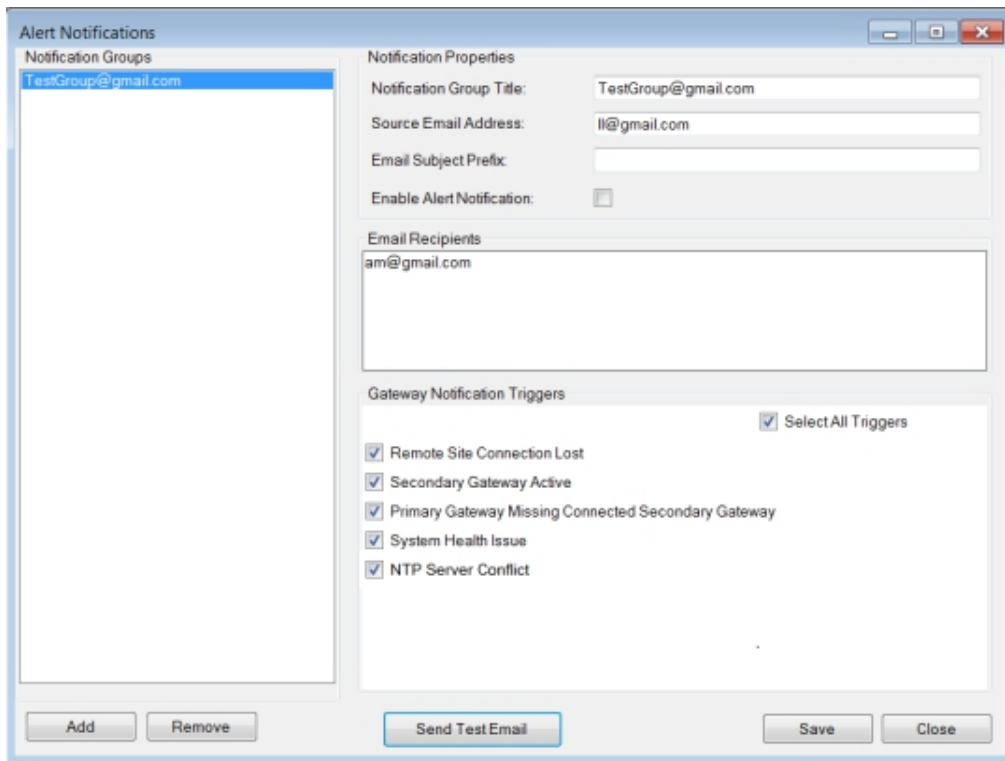
This is the name of the structure used to create and configure an Alert Notification. It is called a Notification Group, because the Alert Notification can be sent to multiple email addresses. Up to five Notification Groups can be created per site, and each Notification Group can be configured for up 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 38: Alert Management Window



Existing Notification Groups are shown in the column on the left. Click an existing group to edit its properties.

7.5.3.1

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.

7.5.4

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.

7.6

Logs

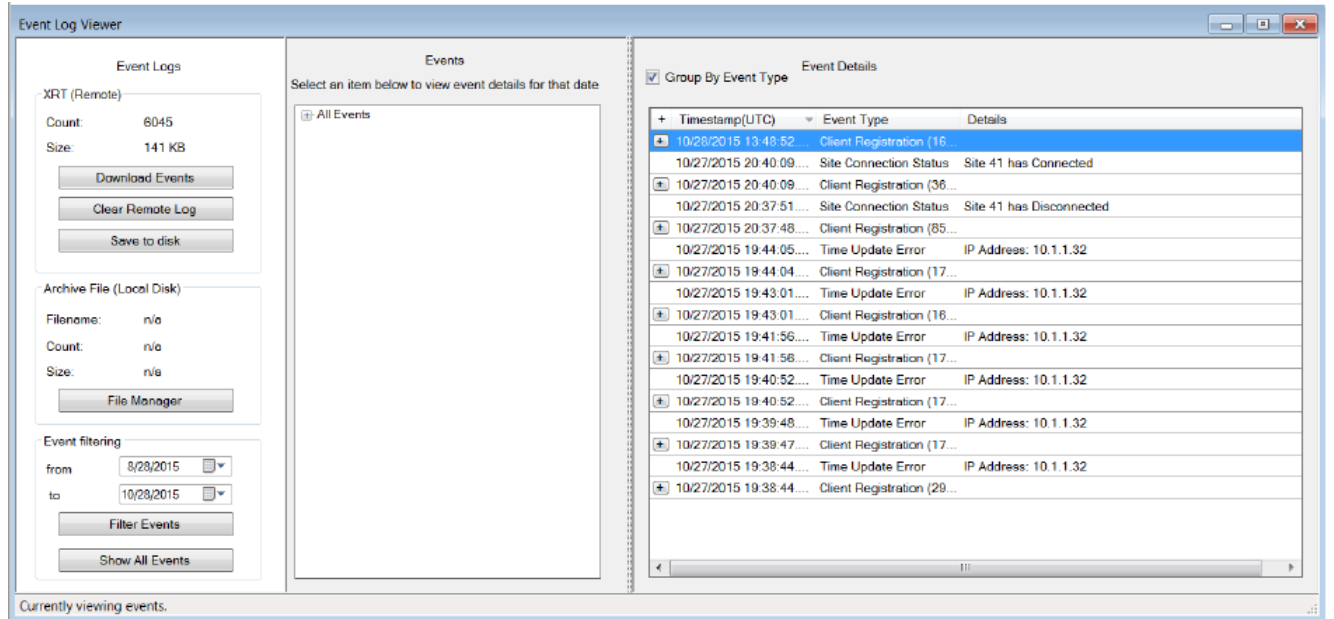
This section explains the viewing and management of various logs.

7.6.1

Event Log Viewer

The event log viewer has three panels: **Event Logs**, **Events** and **Event Details**.

Figure 39: Event Log Viewer Window



Event Logs

Within this panel, event logs are loaded from the device or local PC. Event filtering is also available to aid searching large event logs.

XRT (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

This 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.

Event Details

This 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.

7.6.1.1

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.

7.6.1.1.1

XRT (Remote)

Count displays the number of events currently on the device and Size displays the cumulative file size of all logs 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: download events on a regular schedule and clear the Log after downloading events.

7.6.1.1.2

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.

7.6.1.1.3

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.

7.6.1.1.4

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.

7.6.1.1.5

Archive File (Local Disk)

This area allows access to saved event logs.

Once loaded, **Filename** displays the name of the saved event file, **Count** displays the number of events listed in the loaded file, and **Size** displays the size of the loaded event file.

7.6.1.1.5.1

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.

7.6.1.1.5.2

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.

7.6.1.1.6

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.

7.7

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 and Partial Application Connectivity on page 116 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 116 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. Quantity Available The number of licenses that are still available for the named feature on this Entitlement ID.

Table continued...

	<p>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.</p>
<p>Current Features</p>	<p>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 116 for more information. This section consists of three fields:</p> <p>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 for more information</p> <p>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.</p> <p>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.</p>

7.7.1

Launching the Feature Status Window

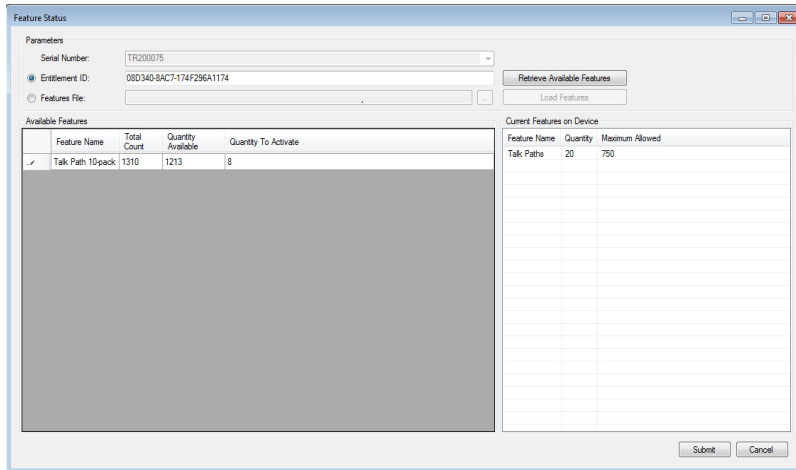
The **Feature Status** window shows the purchasable feature(s) for the connected device, and whether or not any feature on the list is presently enabled. It can also be used to enable additional features for the device.

Procedure:

- 1 From the Menu Bar, select **Settings** → **Features**.

The **Feature Status** window appears. The following example shows the window with full application connectivity after retrieving available features from a valid Entitlement ID. See [Enabling Features with Full Application Connectivity](#) for further information.

Figure 40: Example of Feature Status Window



- 2 When finished, click **X** or **Cancel** to exit the window.

7.7.2

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 112](#) for more information.

7.7.3

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** 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 subsection of [Partial Application Connectivity on page 116](#).



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](#).

7.7.3.1

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 XRT device. The XRT Configuration Tool 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 **Retrieve Available Features**.

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.

When 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

7.7.4

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](#).

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.

7.7.4.1

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 MOTOTRBO Connect Plus XRT Configuration Tool (Connect Plus System Release 1.6 or later) must be installed on the computer.
- The application must be able to access the internet.

Procedure:

- 1 Launch the MOTOTRBO Connect Plus XRT Configuration Tool, but do not connect to the device.

`Not Connected` appears in the lower left-hand corner of the screen.

- 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 entered 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 114](#).
- 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](#).

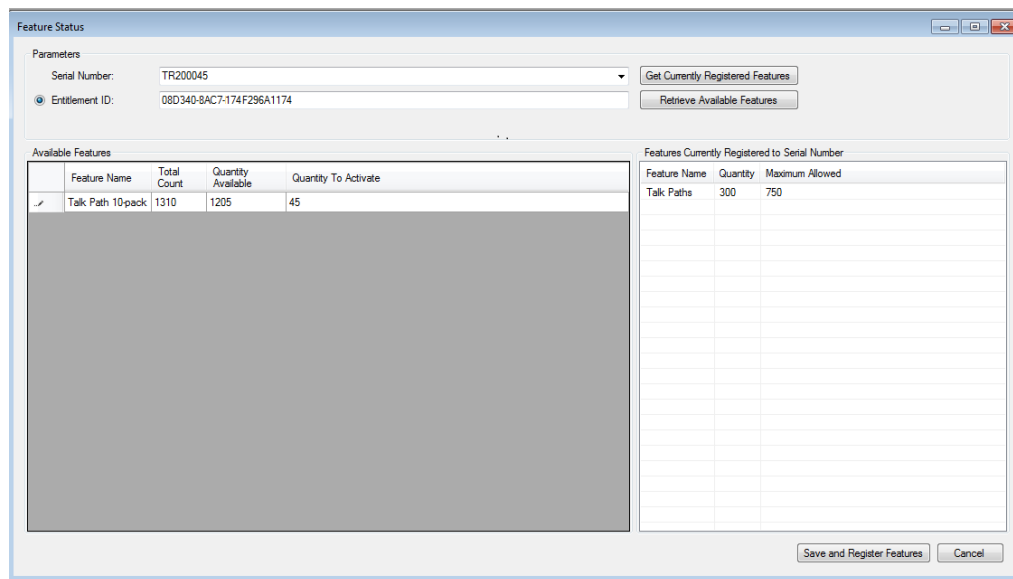
6 Copy the Entitlement ID from the source document and paste it into the **Entitlement ID** field.

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 41: Features Screen in Offline Mode



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 subsection.

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.

7.7.4.2

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 [Connecting to the Features Server and Creating Features Files on page 116](#). The file can only be used with that the device whose Serial Number matches the Serial Number that was entered when the file was created.
- Connect to the desired XRT device.
- Launch the **Feature Status** window.

When and where to use:



CAUTION: Submitting features as described in this section causes the device to reboot.

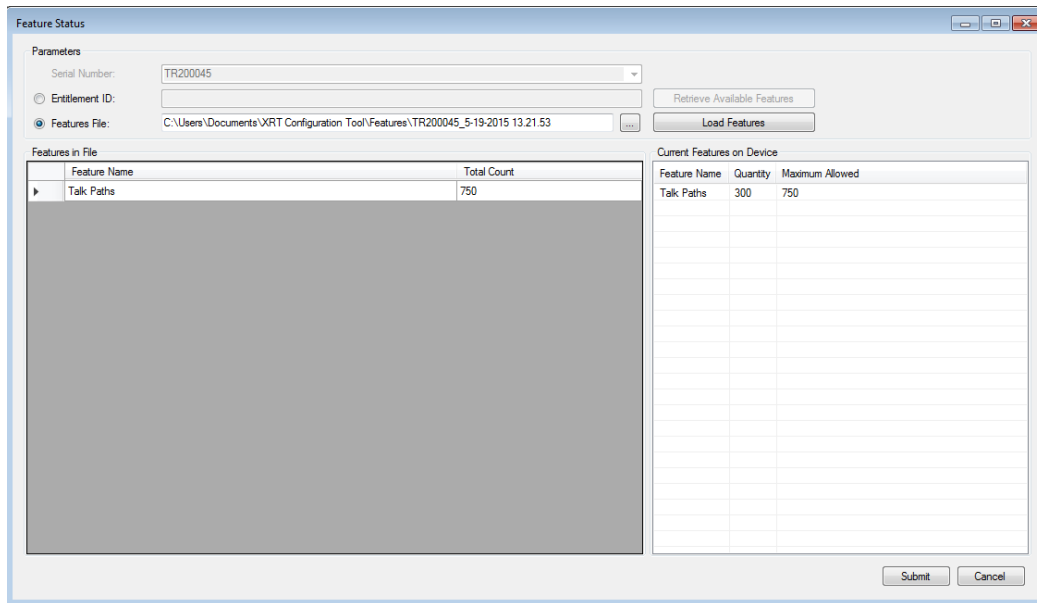
Procedure:

- 1 Click the **Features File** bullet, if not already selected.
- 2 Click the **Browse** icon to launch the **Select a Features File** 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.



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**.

7.8 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 from 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.

7.8.1

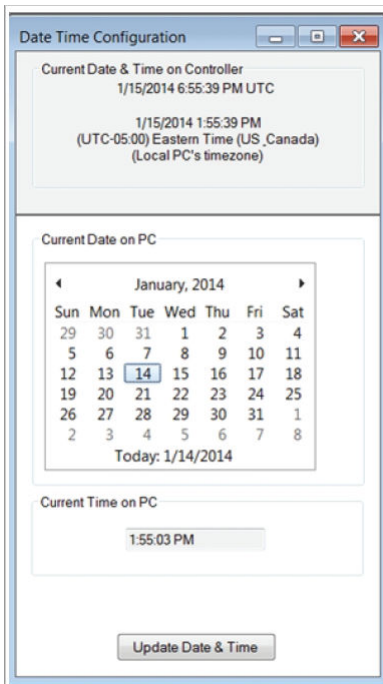
Launching the Date Time Configuration Window

Procedure:

From the Menu Bar, select **Settings** → **Date & Time**.

The **Date Time Configuration** screen appears.

Figure 42: Date Time Configuration Screen



7.8.2

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.

7.9

XRT Configuration Tool Multiple Windows Display Options

7.9.1

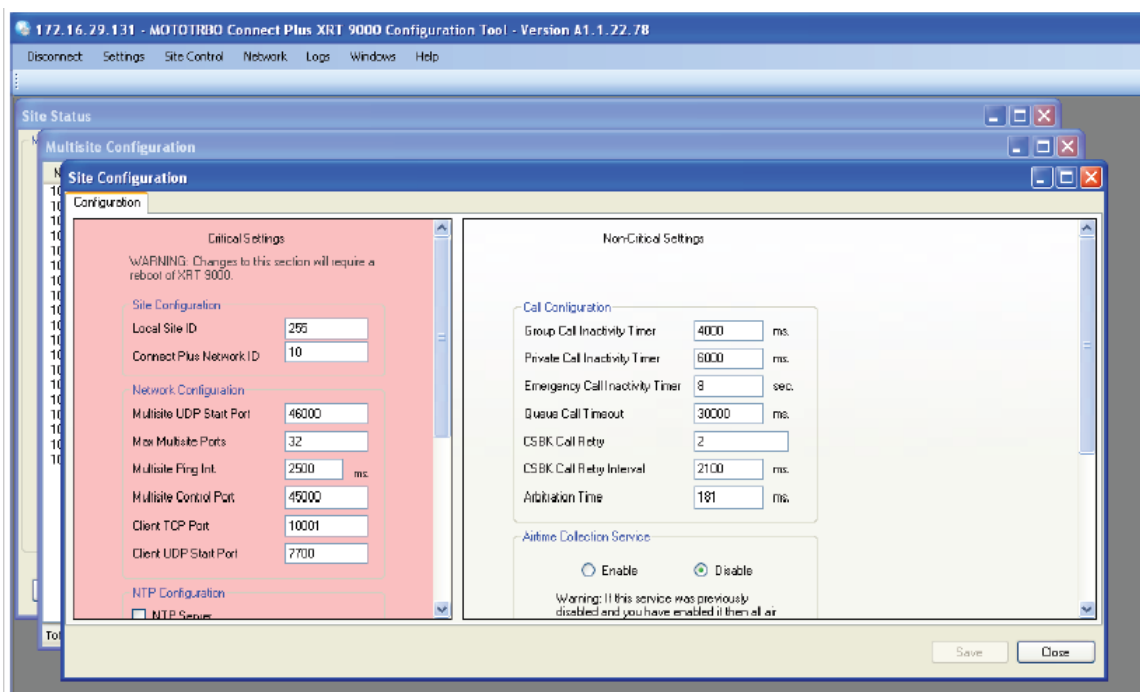
Cascading Windows

This feature allows for all open windows to be cascaded for easy access.

Procedure:

- 1 Have several active windows open within the XRT Configuration Tool.
- 2 From the Menu Bar, select **Windows** → → **Cascade**.

Figure 43: Cascaded Windows

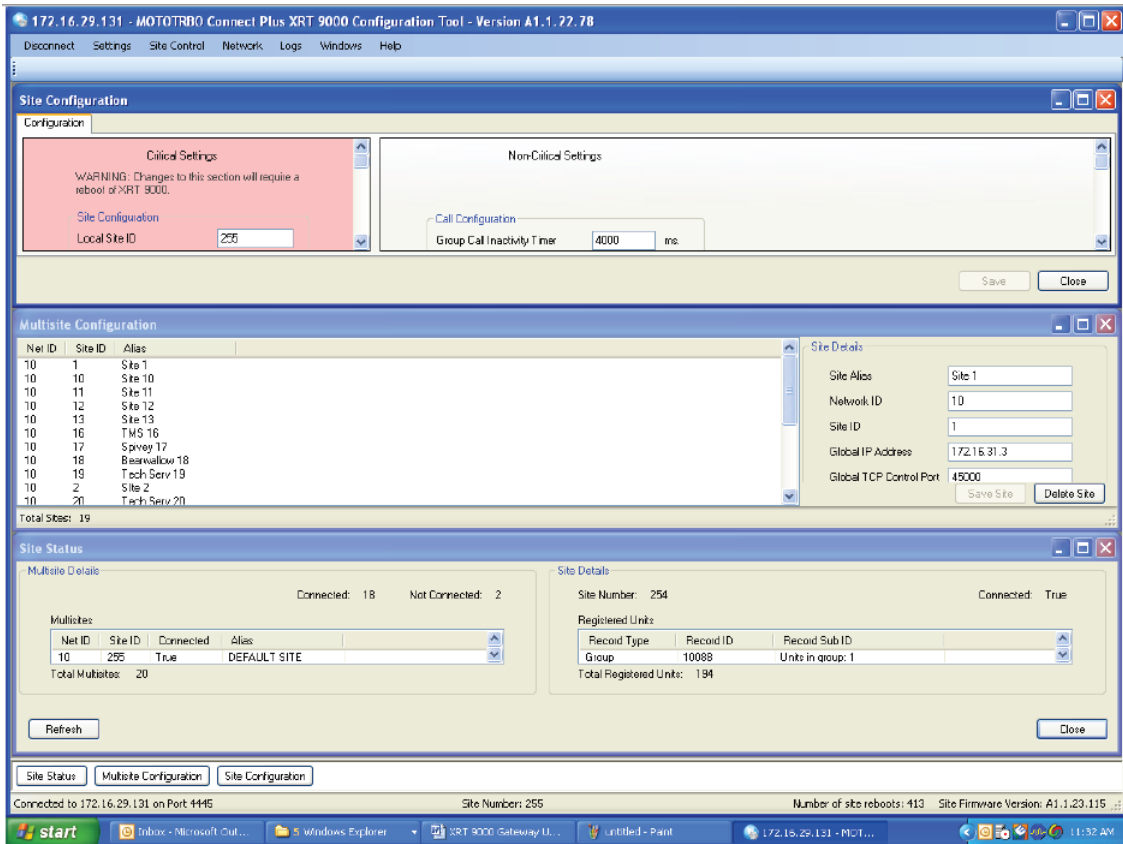


7.9.2 Tiling Windows Horizontally

Procedure:

- 1 Have several active windows open within the XRT Configuration Tool.
- 2 From the Menu Bar, select **Windows** → **Tile Horizontally**

Figure 44: Windows Tiled Horizontally

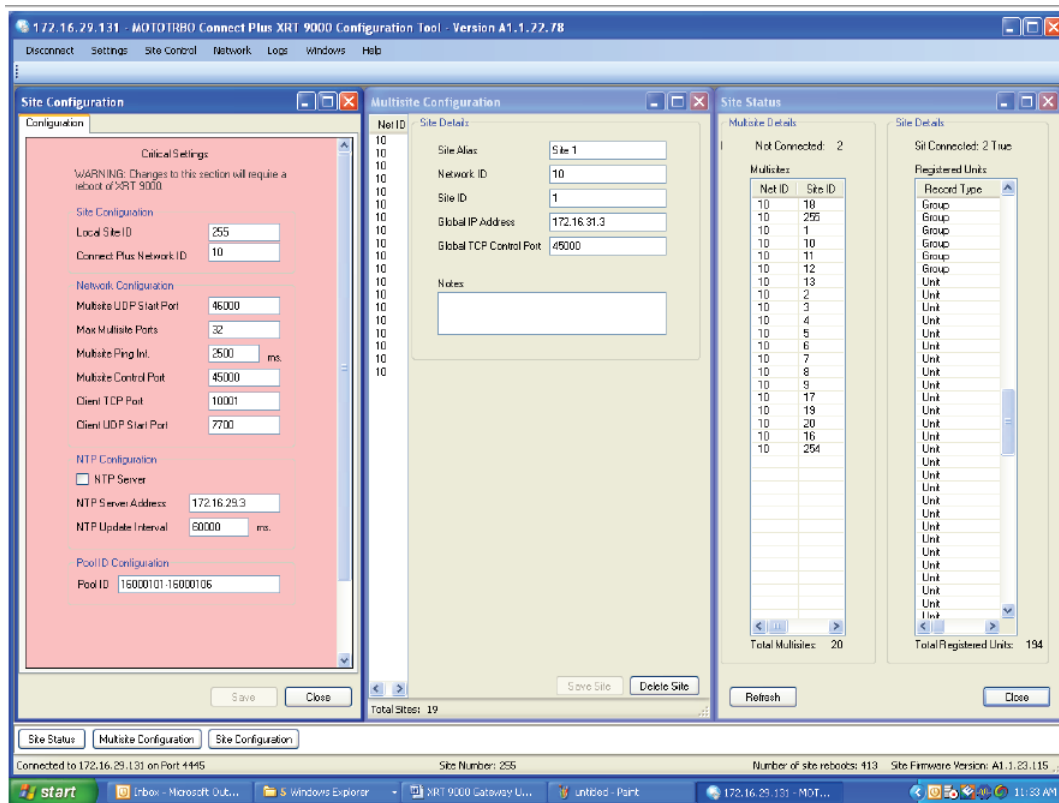


7.9.3 Tiling Windows Vertically

Procedure:

- 1 Have several active windows open within the XRT Configuration Tool.
- 2 From the Menu Bar, select **Windows** → **Tile Vertically**

Figure 45: Windows Tiled Vertically



7.10 XRT User Configuration

A single XRT supports connections from one or more Clients (or "users"). When a Client connects with the XRT, it is required to send a Username and Password combination. This process occurs in the background through messages exchanged between the Client and XRT. The XRT checks to see if the Username and Password sent by the Client can be found in the list of records that have been configured by using the XRT Configuration Tool's User Configuration screen. If the Username/Password combination cannot be found, the Client is not allowed to use XRT resources. If the Username/Password combination is found, then the Client privileges as configured on this screen help determine which features are (and are not) available to the XRT Client.

7.10.1 Creating a New User

Procedure:

- 1 From the Menu Bar, select **Settings** → **XRT User Configuration**
The **User Details** panel is used to enter or edit the user account settings.

Figure 46: User Configuration Screen

The screenshot shows a 'User Details' configuration panel. It contains the following fields and controls:

- Username:** Text input field containing 'admina'.
- Password:** Password input field with masked characters (dots).
- Confirm Password:** Password input field with masked characters (dots).
- Max Talk Paths:** Text input field containing '100'.
- Checkboxes:** Four unchecked checkboxes labeled 'Billing Enabled', 'Network Wide All Call (NWAC) Enabled', 'Data Path Registration Enabled', and 'Configuration Service Enabled'.
- Group Talk Paths:** A sub-panel containing a 'Group ID' text input field.
- Private Talk Paths:** A sub-panel containing a 'Console User ID' text input field.
- Buttons:** Three buttons at the bottom: 'New', 'Save', and 'Delete'.

- 2 Click **New** just below the **User Details** panel.

This places the cursor in the **Username** box within the **User Details** panel.

7.10.2

Entering User Details

Procedure:

- 1 Enter the user details in each field within the **User Details** panel.

Username

The username needs to have a minimum of 5 total characters. Duplicate usernames are not allowed. When the XRT compares the Username configured with the XRT Configuration Tool with the Username sent by the Client, alpha characters (a-z) are case sensitive.

Password

The password needs to have a minimum of five (5) total characters. When the XRT compares the Password configured with the XRT Configuration Tool with the Password sent by the Client, alpha characters (a-z) are case sensitive.



NOTICE: The Password field on this screen does not set the password that is used when logging into the XRT with the XRT Configuration Tool. That password is set on the Change Password screen (**Site Control** → **Change Password**).

Confirm Password

Re-enter the same password with a minimum of five total characters.

Max Talk Paths

Enter the Max number of talk paths and data paths that the user may register. This is the total of all of the following types of paths; Group Talk Paths, Private Talk Paths, and Data Paths.

The total number of talk paths and data paths shared by all users cannot exceed the number of talk paths that have been licensed for this XRT. If the total number of talk paths and data paths of all

users exceeds the number of talk paths licensed for this XRT, a message is provided that shows both the total maximum and currently allocated number of talk paths.

Billing Enabled

Check the box to enable Billing if the user should have access to the Streaming Airtime Data feature.

Network Wide All Call (NWAC) Enabled

Check this box if the user should have permission to register the Network Wide All Call Talk Path.

Data Path Registration Enabled

Check this box if the user shall have permission to register one or more Data Path IDs. A Data Path ID is used to initiate and/or receive packet data calls. On the SU record that corresponds to a Data Path ID in the XRT user database, check the box labeled, **Packet Data Call Enabled**.

Configuration Service Enabled

Check this box if the user is authorized to configure certain settings in connected XRC Controller sites via the XRT Gateway. Also check this box if the XRT User account is for a Capacity Max Bridge (CMB) client. This is required to utilize the CMB's SAC Migration feature.



NOTICE: This feature must also be enabled in the XRT Gateway via the Feature Status screen (unless the connecting client is a Capacity Max Bridge – in which case the feature does not need to be enabled via the Feature Status screen.)

Group Talk Paths:

Leave the **Group ID** field **blank** if the user should have permission for any Group Talk Path that it validly registers with the XRT. If user should have permission to register only specific Group Talk Paths, enter the allowable Group IDs in the **Group ID** field.

IDs may be entered as a range expression (two Group IDs separated by a hyphen) or by listing the allowable Group IDs, separated by commas.



IMPORTANT: If any Group ID is entered, then all Group IDs not configured into this field will be disallowed.

Private Talk paths

Leave the **Console User ID** field **blank** if the user should have permission for any Private Talk Path that it validly registers with the XRT. If user should have permission to register only specific Private Talk Paths, enter the allowable IDs in the **Console User ID** field. IDs may be entered as a range expression (two IDs separated by a hyphen) or by listing the allowable IDs, separated by commas.



IMPORTANT: Do not enter Data Path IDs into this field. If any Private Talk Path ID is entered, then all Private Talk path IDs not configured into this field will be disallowed.

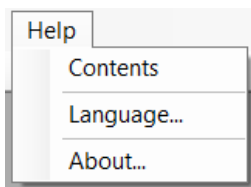
2 Click **Save**.

7.11

Application Help Menu

This application comes with a Help file. The Help file is accessible from the **Help** menu.

Figure 47: Help Menu Drop Down Menu



7.11.1

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.

7.11.2

Selecting the Application Display Language

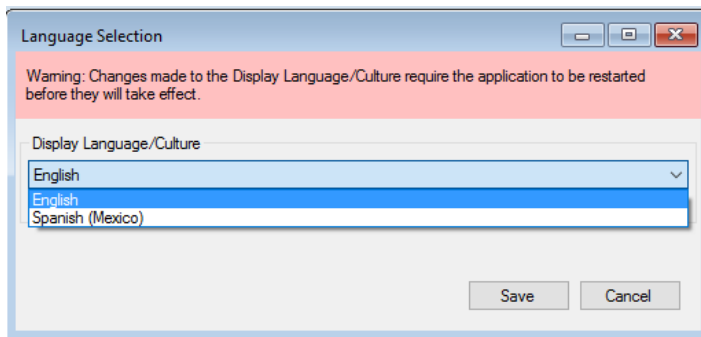
When and where to use: The application can be configured to display in English, or in the same language as the Operating System of the computer (if other than English and supported by the application).

Procedure:

- 1 From the Menu Bar, select **Help** → **Language ...**

The **Language Selection** screen appears.

Figure 48: Language Selection Screen



- 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.

7.11.3

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.

This page intentionally left blank.

Chapter 8

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.