



RoamAlert®

**System
Installation
Manual**

Xmark®
Know for sure

Xmark Corporation
309 Legget Drive, Ottawa, ON K2K 3A3, Canada
Telephone: 1.866.55XMARK
International: +1 (613) 592.6997
Facsimile: (613) 592.4296
Web Site: www.xmark.com
E-mail: support@xmark.com

Certified to the ISO 9001 Quality Standard

© 2006 - 2008 Xmark Corporation. All Rights Reserved. RoamAlert and Xmark are registered trademarks of Xmark Corporation Inc. in North America. All other company and product names may be trademarks of their respective companies. Printed in Canada. January 2008. 981-000043-000 R04.

Warranty

Xmark's products are warranted against defects in materials and workmanship and shall perform in accordance with published specifications for the following periods:

- Infrastructure components (receivers, door and elevator controllers, keypads, exciters, etc.) – 2 years,
- Wrist and staff tags with pulse technology – 1 year, and
- Asset tags and wrist tags without pulse technology – 3 years.

Xmark's warranty is limited solely to the repair or replacement of the defective part or product. Xmark reserves the right to change product specifications without notice.

Limitation of Liability

This Product has been designed for use to: a) assist personnel in summoning help when they are under personal duress, b) locate assets c) assist in the prevention of the loss of assets and/or d) reduce the risk of resident wandering through remote detection.

The range, accuracy, function and performance of this Product may vary from the published specifications due to many factors, including, without limitation, site impairments from structural effects, metal objects in the vicinity, placement of the receiver and transmitter, interference from other electrical devices, atmospheric effects, installation, and maintenance. There may be other factors, which also affect performance of this Product.

Xmark Corporation does not guarantee that this Product will: a) detect 100% of the calls for personal assistance, b) locate all assets 100% of the time, c) prevent the loss of assets and/or d) detect 100% of resident wanderings. Xmark does not guarantee that this Product will not return false reports of: a) calls for personal assistance, b) location of assets, c) loss of assets and/or d) false reports of resident wandering.

Monthly testing and maintenance of this Product, as described in the Product documentation, is essential to verify the system is operating correctly and to ensure that the probability of detecting an alarm and/or locating the transmitter are maximized.

The failure to undertake regular testing and maintenance will increase the risk of system failure and: a) failure to report personal duress calls, b) failure to locate assets, c) failure to prevent the loss of assets and/or d) failure to detect resident wandering. The failure to undertake regular testing and maintenance will increase the risk of false reports of: a) calls for personal assistance, b) location of assets, c) loss of assets and/or d) resident wandering.

Xmark hereby disclaims all warranties, express or implied, arising out of or in connection with any of its Products of the use or performance thereof, including but not limited to, where allowable by law, all other implied warranties or conditions of merchantable quality and fitness for a particular purpose and those arising by statute or otherwise in law or from a course of dealing or usage of trade.

Xmark's liability to you or anyone claiming through or on behalf of you with respect to any claim or loss arising out of the use or misuse of Xmark's Product, defective products or materials, improper installation or maintenance of Xmark's Product or products or the system in which they are incorporated, or alleged to have resulted from an act or omission of Xmark or any person, negligent or otherwise, shall be limited to:

A) the repair or replacement of defective Product or materials supplied by Xmark during the warranty period as set out in the Product documentation; or, at the option of Xmark,

B) a refund of the purchase price of the Product supplied by Xmark.

In no event shall Xmark be liable for general, specific, indirect, consequential, incidental, exemplary or punitive damages or any losses or expenses suffered by you or anyone else, whether or not Xmark, or its employees, officers, agents, resellers or installers has been informed of the risk of such loss or expense and whether or not such losses or expenses were foreseeable.

UL Listing

This system is listed as an Access Control System by Underwriters Laboratories Inc., Standard for Safety.

Warnings

Please observe the following warnings when using the RoamAlert system.

- Wire mesh can severely affect the operation of the RoamAlert system – wire mesh, foil-backed ceiling tiles, and other metal barriers in walls and ceilings interfere with radio frequency transmission and reception. The RoamAlert system may not operate properly in facilities where these materials are used.
- The RoamAlert system does not incorporate an emergency power supply circuit. As a result, residents will not be protected in the event of a general power failure.

RoamAlert Tags

- No user adjustments – there are no user adjustments. Tampering with the internal circuitry may cause component or system failure, or both, and will void the warranty.
- Battery handling – this device contains a lithium battery. Do not force open, heat to 100° C, or dispose of in fire.
- X-rays – do not directly expose the tag to X-rays. (The tag is not affected by stray radiation.)

Receivers

- Electrostatic discharge could damage the receiver and internal components—touch your hand to ground to discharge any electrostatic charge before wiring the receiver.
- No user adjustments – there are no user adjustments. Tampering with the internal circuitry may cause component or system failure, or both, and will void the warranty.
- Follow installation instructions precisely – instructions must be carefully followed throughout the installation of all receivers. Failure to follow the instructions may cause degraded performance.

Door and Elevator Controllers

- Electrostatic discharge could damage the controller's internal components—touch your hand to ground to discharge any electrostatic charge before wiring the controller.
- No user adjustments – there are no user adjustments. Tampering with the internal circuitry may cause component or system failure, or both, and will void the warranty.
- Follow installation instructions precisely – instructions must be carefully followed throughout the installation of all controllers. Failure to follow the instructions may cause degraded performance.
- The elevator controller is UL listed as elevator equipment – The fire control panel shall override the controller when the latter is wired to an elevator control system.
- Ensure the fire control panel has control over all magnetic door locks interfaced to the controller. Install door locks in fail-safe mode so that they release upon loss of power or loss of connection to the fire control panel.

Server and Console PCs

- Do not operate other software programs at the same time as the RoamAlert system software - do not use these or other software:
 - Disk compression – disk compression technology is not recommended.
 - Back up programs – back up programs, including the Microsoft® Windows® back up program, warn of problems when continuing to use the system during a backup. Also, the system does not support the use of a tape drive. Exit the server PC software before starting a back up session.
- Turn off power management for all computers used in the RoamAlert system – power management can interfere with the proper operation of the RoamAlert system software.

FCC and IC Regulatory Statements

The following statements apply to the RoamAlert tag, receiver, controller, and exciter.

United States – Federal Communication Commission (FCC)

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference 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 his own expense.

Warning: Changes or modifications not expressly approved by Xmark could void the user's authority to operate the equipment.

Canada – Industry Canada

This device complies with RSS-210 of Industry and Science Canada. Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Software License Agreement

This is a legal agreement between you (either an individual or an entity) and Xmark Corporation ("Xmark"). By opening the sealed disc envelope you are agreeing to be bound by the terms of this agreement. If you do not agree with the terms of this agreement, promptly return the unopened disk envelope and the accompanying items (including user manuals and other written materials) to the location where you obtained them.

The software which accompanies this license agreement (the "Software") is warranted against defects in materials and workmanship and shall perform substantially in accordance with the accompanying written materials for a period of one year. Should a product fail within this period it shall be repaired or replaced free of charge. Xmark does not warrant that the operation of the Software will be uninterrupted or error free. Xmark does not represent that any product will prevent bodily injury or damage to property. This warranty is void if the product has been dismantled, altered or abused in any way. EXCEPT FOR THE WARRANTIES SPECIFIED IN THIS AGREEMENT, THERE ARE NO WARRANTIES OR CONDITIONS, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO WARRANTIES OR CONDITIONS OF FITNESS FOR PURPOSE, MERCHANTABILITY OR FUNCTION OF THE SOFTWARE FOR A PARTICULAR PURPOSE AND THOSE ARISING BY STATUTE OR OTHERWISE IN LAW OR FROM A COURSE OF DEALING OR USAGE IN TRADE. USE OF THE SOFTWARE IS ENTIRELY AT YOUR SOLE RISK.

XMARK WILL NOT BE LIABLE FOR: (A) HARM TO OR LOSS OF YOUR RECORDS OR DATA; (B) ANY CLAIMS AGAINST YOU BY THIRD PARTIES; OR (C) ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, INCLUDING BUT NOT LIMITED TO LOST PROFITS, LOST BUSINESS REVENUE, OR FAILURE TO REALIZE ON SAVINGS, EVEN IF XMARK HAS BEEN ADVISED OF THE POSSIBILITY OF THESE DAMAGES. THIS LIMITATION APPLIES TO ALL CLAIMS BY YOU IRRESPECTIVE OF THE CAUSE OF ACTION UNDERLYING THE CLAIM BUT NOT LIMITED TO BREACH OF CONTRACT INCLUDING FUNDAMENTAL BREACH, TORT INCLUDING NEGLIGENCE AND MISREPRESENTATION; AND BREACH OF STATUTORY DUTY. IN NO EVENT SHALL THE LIABILITY OF XMARK EXCEED THE COST OF THE SOFTWARE.

This agreement allows you to use the Software on the Xmark locating or monitoring system (the "System") in the facility or premises in which the System is installed by Xmark or its dealer(s), and make copies of the software solely for backup purposes. You must reproduce on any such copy all copyright notices and any other proprietary legends on the original copy of the Software. You may not decompile, reverse engineer, disassemble, or otherwise reduce the Software to a human conceivable form.

The Software and the rights herein are not transferable except: (i) to other facilities or locations in connection with a transfer of the System that is approved in writing by Xmark, in its sole discretion; or (ii) in connection with the transfer of ownership of the facility in which the System is installed, provided that the System is not altered thereby. Although you own the disk on which the Software is recorded, you do not become the owner of, and Xmark retains title to, the Software, and all copies thereof. All rights not specifically granted in this agreement are specifically reserved by Xmark.

Xmark may terminate your license if you breach any term of this agreement and do not remedy the breach within 10 days written notice of the breach. Upon termination you will immediately delete the Software from the computer in which it is installed and return all copies of the Software to Xmark.

This agreement constitutes the entire agreement of the parties with respect to the subject matter and supercedes all prior agreements, understandings, negotiations and discussions, whether oral or written, between the parties. This agreement will be governed by the laws of the Province of Ontario excluding the law of conflicts and excluding the United Nations Convention of Contracts for the Sale of Goods. You agree to attorn to the exclusive jurisdiction of the courts of the Province of Ontario which will have exclusive jurisdiction over matters in respect of this agreement.

CONTENTS

Warranty.....	i-iii
Warnings.....	i-iv
FCC and IC Regulatory Statements.....	i-v
Software License Agreement.....	i-vi

Introduction 1-1

Manual Organization.....	1-1
What is the RoamAlert System?.....	1-2
RoamAlert Tags.....	1-3
Basic System Components.....	1-4
Server and Consoles.....	1-4
Hardware.....	1-4
RoamAlert Software.....	1-4
Paging Interface.....	1-4
Door Control System.....	1-4
Controller with Receiver.....	1-5
Receivers.....	1-6
24 VDC Power Supply.....	1-7
Pocket Tag Reader.....	1-7
Optional System Components.....	1-8
Elevator Control System (with RS485 Repeater).....	1-8
Elevator Hardware.....	1-8
I/O-8 Interface Module.....	1-9
Wiegand Interface.....	1-10
Network Manager (NM).....	1-10
Remote Display Unit (RDU).....	1-10

System Design 2-1

Theory of Operation.....	2-2
About RF Interference.....	2-2
System Design Overview.....	2-3
Assessing the Facility.....	2-4
Physical Environment.....	2-4
Radio Frequency Environment.....	2-4
Exit Requirements.....	2-5
Usability Requirements.....	2-5
Testing for RF Noise.....	2-6
Ambient VHF Noise Testing.....	2-6
Ambient LF Noise Testing.....	2-6
Planning the Location of Controller Systems.....	2-7
Exciter Placement.....	2-7
Controller System Layout.....	2-10
Creating a Coverage Plan.....	2-11
Locating Receivers on the Coverage Plan.....	2-12
Planning the RS-485 Network and Power Distribution.....	2-14
Network Communications.....	2-14

Topology	2-14
Network Design Considerations	2-14
Good Wiring Practices	2-15
Cable Specifications	2-15
Power Distribution	2-15
Design Considerations.....	2-16

Hardware Installation 3-1

General Installation Tips	3-2
Installing Power, Wiring and Network Cabling	3-3
Installing the Central Power Supply and Wiring	3-3
Installation Tips	3-3
Installation Procedures	3-3
Installing the RS-485 Network Cabling.....	3-3
Installation Tips.....	3-3
Installing and Testing the Door Control System.....	3-4
Door Controller Installation Tips.....	3-4
Exciter Installation Tips.....	3-4
Receive Antenna Installation Tips.....	3-5
Door Controller and Exciter Installation Procedure	3-5
Controller Connection Notes and Diagrams	3-6
Connecting a Third-Party Keypad.....	3-10
Installing a Magnetic Door Switch.....	3-11
Door Switch Installation Tips.....	3-11
Door Switch Installation Procedure	3-11
Door Switch Notes and Diagrams	3-12
Installing a Maglock	3-13
Maglock Installation Tips.....	3-13
Maglock Installation Procedure	3-13
Installing a Keypad	3-15
Keypad Installation Tips.....	3-15
Keypad Installation Procedure.....	3-15
Mode 2 Passcode Programming Procedure.....	3-16
Keypad Notes and Diagrams.....	3-17
Installing a Wiegand Interface	3-18
Wiegand Interface Installation Procedure.....	3-18
Wiegand Interface Notes and Diagrams.....	3-19
Installing and Testing Receivers	3-21
Receiver Installation Tips.....	3-21
Receiver Installation Procedure.....	3-21
Receiver Notes and Diagrams.....	3-23
Installing and Tuning Elevator Control Systems	3-25
Elevator Control System Overview.....	3-25
System Layout.....	3-26
System Operation	3-26
Elevator Control System Installation Tips	3-27
Elevator Control System Installation Procedures	3-28
Controller, Keypad, Wiring and Receive Antenna Installation	3-28
Permanently Mounting the Exciters	3-32
Elevator System Notes and Diagrams.....	3-33

Installing an I/O-8 Module	3-38
I/O-8 Module Installation Tips	3-38
I/O-8 Module Installation Procedure	3-39
I/O-8 Module Notes and Diagrams	3-40
Installing an Alarm Output Module	3-42
Alarm Output Module Installation Tips	3-42
Alarm Output Module Installation Procedure	3-43
Alarm Output Module Notes and Diagrams	3-44
Installing a Remote Display Unit (RDU)	3-45
RDU Installation Tips	3-45
RDU Installation Procedure	3-46
RDU Configuration	3-47
Settings at the RoamAlert Server PC	3-47
Settings at the RDU	3-47
RDU Notes and Diagrams	3-51
Operating Modes	3-51
LED Display	3-52
Audible Alarms	3-52
RDU Communications with the RoamAlert Server	3-52
Molex Connector	3-53
Cable Requirements	3-53
Installing a Network Manager	3-54
Network Manager Installation Tips	3-54
Network Manager Installation Procedure	3-54
Removing the Termination Jumpers	3-55
Network Manager Notes and Diagrams	3-56

Software Configuration **4-1**

Installing the RoamAlert Software	4-2
System Access Levels	4-5
Configuring RoamAlert Software	4-6
Change the RS-485 Network Port	4-7
Set Global Configuration Options	4-10
Configuring RDU Audible Alert Profiles	4-12
Add and Configure Nodes	4-13
Add and Configure Consoles	4-19
Add Floor Plans	4-24
Place Nodes on Floor Plans	4-27
Add Users and Set Access Levels	4-29
Add Tags to Inventory	4-32
Add and Configure Tag Categories	4-40
Add Annotations	4-43
Configure Alarm Sounds	4-45
Add and Configure Messaging Devices	4-48
Add Links	4-50

System Commissioning **5-1**

Performing the Final System Check	5-2
Door Controllers	5-2
Elevator Controllers	5-2
Documenting the Installed Software and Hardware	5-3

Software	5-3
Hardware	5-3
Door Controllers.....	5-3
Elevator Controllers	5-3
Receivers.....	5-3
Delivering the System to the Client.....	5-4
Commissioning Forms	A-1
Importing User Records	B-1
R3 Receiver Installation	C-1
Creating a Receiver Coverage Plan	C-2
Locating Receivers on the Coverage Plan	C-3
Testing Receiver Coverage.....	C-4
Index	I-1

INTRODUCTION

This manual provides instructions on how to install, configure, and commission a RoamAlert wander prevention system. It is intended for the trained installer who is familiar with wiring in commercial and industrial facilities, micro-electronics including static-sensitive components, and computers.

This chapter introduces you to the:

- organization of the manual,
- purpose of the RoamAlert system,
- basic components and layout of a RoamAlert system, and
- optional components that may be required in certain facilities, or that enhance the system.

Manual Organization

This installation manual is organized into five main sections:

- **Introduction** – the section you are reading now, which introduces the RoamAlert system and its basic and optional components.
- **System Design** – this section presents the theory of RoamAlert operation and provides instruction and guidance for the planning and design of a system.
- **Hardware Installation** – this section provides detailed technical instructions for installing the RoamAlert system components.
- **Software Configuration** – this section describes RoamAlert software configuration.
- **System Commissioning** – this section covers the final testing that is performed to commission the system and deliver it to the client.

Important:

Failure to thoroughly consider in advance all aspects of system design can mean many frustrating hours adjusting device locations or re-routing power and network cabling.

What is the RoamAlert System?

The RoamAlert Wander Prevention System is an electronic system which, in conjunction with staff diligence, helps create a secure perimeter to deter wander incidents from a specific area. Within this perimeter, an optional set of receivers can detect tags and can locate tagged residents, staff and movable assets.

Residents protected by the RoamAlert system are tagged with a Xmark transponder called a **Tag**. RoamAlert can secure the perimeter of areas such as a floor, a wing, common areas, etc.

The perimeter protection and tag location is accomplished in two basic ways:

- Controllers installed at each exit detect the presence of tags and can generate alarms and lock doors, and
- Receivers placed throughout the safe area detect tags and can locate a tag within the area.

In a typical application, the residential wing of a long-term care facility is defined as a “safe area.” Within this area, residents may move freely. Exits from the safe area are equipped with Controllers mounted at the doorways. As a resident approaches a Controller, the tag sends a special signal to identify itself. This information is relayed to the Server PC, where a warning or alarm message is automatically generated and the door is locked.




There are two types of wrist tags; standard (blue) and pulse technology (green). The tag is enrolled into the system when it is assigned to the resident. From the moment it is activated, the tag protects the resident. Blue and green tags emit signals when they approach a controller. Green tags also emit a pulse every 16 seconds. Receivers monitor these pulses and the RoamAlert server PC generates an alarm if the pulse is not detected after a specified (configurable) period.

Residents can leave the safe area for legitimate purposes (e.g., testing, to go home for the weekend, etc.). The tag is “Transported” out of the system for a set time at the server or console PCs. If the tag is not detected by the system after the transport time has expired, an alarm can be automatically generated.

The RoamAlert system employs a network based on the RS-485 protocol. The server PC is connected over the network to every controller and receiver, along with optional devices such as I/O modules. All devices are continually supervised, and an alarm is automatically generated if communication is lost.


The RoamAlert system is modular in design, providing flexibility during installation, and easy expansion. Small systems can be enlarged to cover larger areas, or to add other applications.

RoamAlert Tags

Tag	Description
All Tags	<ul style="list-style-type: none"> • are transponders that transmit at 433.92 MHz and receive at 307 KHz., • are encoded with a unique electronic serial number, • have a circuit that transmits an alarm when the battery is depleted.
Wrist Tag	
	<p>The wrist tag provides protection to residents. The tag also generates an exit alarm (TIF) if it is brought near a protected exit. The wrist tag is worn on the resident's wrist and is attached using a tear-proof band.</p> <p>The green wrist tag has tag pulse technology that sends a location signal every 16 seconds.</p>
Staff Tag	
	<p>Staff tags can be configured so that the system automatically bypasses doors when the staff member enters a door controller's detection zone with a tagged resident (auto bypass). The staff tag also has a "panic" button that can be pressed to generate an alarm during duress situations.</p>
Asset Tag	
	<p>Asset Tags are used to protect mobile assets such as IV pumps, crash carts, monitors, etc. Once an asset tag is affixed to an asset, any unauthorized attempt to remove the tag will result in an alarm. RoamAlert also generates an alarm if the tag is brought near a protected exit. Like the green wrist tags, the asset tag has pulse technology which allows the facility to accurately track and locate tagged equipment.</p>

Basic System Components

Server and Consoles

Component	Description
RoamAlert Server or Console	
	<p>The server PC and console PCs are the computers that control the RoamAlert system. The application software and central database resides on the server PC, which receives status information from the door controllers, elevator controllers, and receivers via an RS-485 network. The server PC can be connected to one or more console PCs over a standard local area network (LAN), so that system activity can be monitored from several different locations in the facility. At a console PC, non-administrative software functions can be accessed.</p> <p>Although the server PC is used to initially configure the system, it can also be used on a day-to-day basis since all console PC functions are available at the server PC.</p>

Hardware

Xmark can supply all computer hardware (except the PC monitor) as part of plug-in server and console bundles. Plug-in server bundles include the PC with RoamAlert software fully integrated, keyboard, mouse, Tag Link with cables, RF Test Tag, Pocket Tag Reader and P4 Tag Rack. Plug-in console bundles include the PC with RoamAlert software fully integrated, keyboard, mouse, and Tag Link with cables.

Self-install server bundles include the software CD, external RS232/485 converter, Tag Link with cables, RF Test Tag, Pocket Tag Reader and P4 Tag Rack. For self-install consoles, Xmark supplies a RoamAlert software CD workstation license.

RoamAlert Software

The current software release is 1.4. It is supplied on CD and is installed on the server and all console PCs. Check with Xmark for updates.

Paging Interface

RoamAlert software includes a paging interface that allows alarm event notification to be sent directly in real time to a messaging device (e.g. a pager or wireless handset that can display text messages).

Staff within range of the facility's internal paging system can receive instant alarm notification without having to be close to a RoamAlert console. Individual messaging devices can be configured to receive only those alarms from specific consoles that are relevant to a particular staff member or staff group.

Door Control System

The basic door control system includes these components:

- one controller,
- one receive (RX) antenna,
- one SRA exciter antenna with cable,
- one access keypad with cable,

- two magnetic door switches with screws and cables, and
- associated cables (for door switch and exciter).

Depending on physical and environmental characteristics, or functionality required by the client, the door control system may also include:

- a second keypad and associated cable,
- a second exciter and cable,
- a second door switch with screws and cable,
- one or two maglocks,
- a Wiegand interface,
- the connection of other equipment such as call system annunciators or fire alarm systems.

Controller with Receiver

The controller is the heart of the RoamAlert perimeter system. It generates an exciter field (through an attached exciter antenna), which defines the area within which a tag generates an exit alarm. If an exit alarm is detected, the controller can activate a maglock to hold the door shut. The controller also contains a receiver which can detect off-body (TIC) alarms generated when a tag is removed from an asset within range. The receiver also detects tag location messages (TLM).

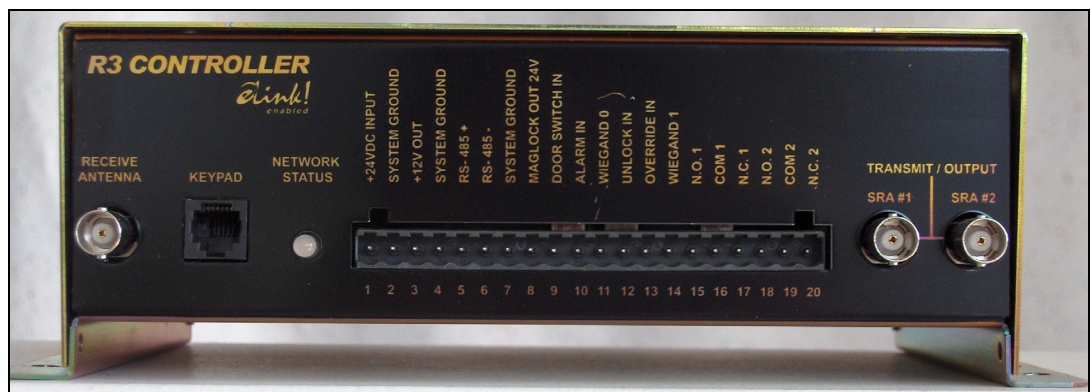







Figure 1-1: R3 Door Controller Front Panel



Door Controller Subsystem Hardware

Component	Description
Exciter Antenna	
	The exciter antenna creates an electromagnetic field at an exit, tuned to 307 KHz, that activates tags entering the field. The exciter antenna is typically mounted above the drop ceiling or inside the wall at a doorway. Two antennas may be used with a controller to provide coverage for exits up to 20 feet wide.
Receive Antenna	
	The receive antenna is attached to the controller front panel with the supplied BNC connector. The antenna orientation can be adjusted so that it remains vertical no matter the position of the controller. In cases where the controller must be mounted above a metal pan or foil-backed ceiling tiles, the elevator receive antenna can be used for appropriate positioning.
Magnetic Door Switch	
	The magnetic door switch is used to detect whether the door is open or closed. Two switches and cables are supplied to accommodate double door installations.
Access Keypad	
	The access keypad is installed near a door, usually outside the exciter field. You enter a code to temporarily bypass the controller, allowing a tag to enter the exciter field without generating an alarm. The keypad also provides an audible and visual indication of alarm conditions as well as standby, bypass, and power-on conditions.


Receivers

Component	Description
R4 Receiver	
	The receiver monitors and receives tag messages such as TIC alarms and tag location messages (TLM) that occur in areas outside the detection zone of a controller. The receiver is a compact, unobtrusive device usually mounted out of sight in areas such as drop ceilings. Enough receivers are placed throughout the secure area to ensure complete coverage.

24 VDC Power Supply

Component	Description
<p data-bbox="386 310 641 338">CPS 24 Power Supply</p> 	<p data-bbox="673 352 1463 516">The CPS 24 is a central power supply designed to work with the R3 Controller and allows for the connection of Maglocks. It converts 115 VAC 50/60Hz input into eight (8) independent, fuse protected, 24 VDC trigger controlled outputs and also offers 10A continuous supply current. The form "C" dry output relay enables Alarm Monitoring, HVAC Shutdown, and Elevator Recall; the relay can also be used to trigger auxiliary devices.</p> <p data-bbox="673 527 1463 627">Each fuse-protected output can route power to a variety of access control hardware and devices such as Maglocks, Electric Strikes, Magnetic Door Holders, etc. These outputs can operate in either fail-safe or fail-secure modes.</p>
<p data-bbox="386 642 571 669">Gel 6.0 Gelpack</p> 	<p data-bbox="673 684 1463 848">The Gel 6.0 Battery is a rechargeable sealed lead-acid battery used in the CPS24 to provide power to the system in the event of a power failure. The CPS24 has sufficient space for two Gel 6.0 batteries. The amount of time the batteries will last during a power failure is dependent on the current draw from the batteries. The batteries are charged by the CPS 24 and should be replaced at two-year intervals.</p>

Pocket Tag Reader

Component	Description
<p data-bbox="386 1033 522 1060">Tag Reader</p> 	<p data-bbox="673 1075 1463 1155">The tag reader is a hand-held device used to perform basic tests and to program tags whether or not they are attached to residents. The reader has an internal low battery indicator.</p> <p data-bbox="673 1165 1463 1245">In user mode, the reader can determine a tag's serial number, warranty expiry date, battery status and whether the tag supports location messages (TLM). The reader can also test a controller's field and check for RF noise.</p> <p data-bbox="673 1255 1463 1283">In technician mode, the reader can read, test and configure tags.</p> <p data-bbox="673 1293 1463 1320">Refer to the Tag Reader User Guide for complete details and instructions.</p>


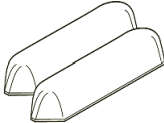

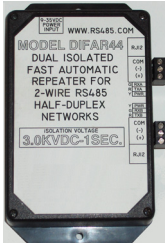
Optional System Components



Elevator Control System (with RS485 Repeater)

The elevator system controls the operation of a facility's elevators. Instead of lobby coverage on every floor, the elevator system travels with each elevator car, containing the detection field within that car.


The elevator controller initiates a pre-alarm in an attempt to clear unauthorized people from the elevator car without staff intervention. If the keypad mounted on the elevator control panel is activated before the pre-alarm has ended, the elevator enters bypass mode, which allows normal operation. Otherwise, the system generates an alarm, holding the elevator doors open until the tag is removed from the car.

Elevator Hardware


Component	Description
Controller and Cabinet	
	<p>The R3 Elevator Controller looks like a door controller placed inside a box with sirens and switch inputs added. However, specialized firmware causes the elevator controller to behave much differently. Therefore, door and elevator controllers are not interchangeable. When a tag enters the elevator car, the controller can cause the elevator doors to be locked open until the tag leaves the car or the keypad is used to bypass the interface.</p>
SRA-E Exciter Antenna	
	<p>These surface-mounted exciters create an electromagnetic field, tuned to 307 KHZ, that activates tags entering the elevator car. Two antennae are typically mounted below the handrail on each side of the car and then adjusted to contain the field within the car.</p>
Receive Antenna and Cable	
	<p>The elevator receive antenna is attached to a 15-foot RG58 coaxial cable with a BNC or F-type connector to connect the antenna to the controller. The antenna portion is housed in a plastic case that is mounted to any non-metallic surface with the supplied double-sided tape. The elevator antenna may also be used in situations where door controllers must be mounted above metal pans or foil-backed ceiling tiles.</p>
RS-485 Repeater	
	<p>This is a dual optically isolated fast automatic repeater. It allows a network to be extended further than 4000', and provides isolation when used for elevator installations and high risk areas, compensating for network deficiencies.</p> <p>As a network extender, up to 2 repeaters can be used to extend the RS-485 network beyond its normal 4,000 foot limit.</p> <p>As elevator isolation drivers, up to 5 repeaters can be used. Each repeater can isolate up to 3 elevator controllers.</p>

Component	Description
Access Keypad 	<p>The access keypad is installed inside the elevator car. When a tag enters the car's exciter field, a pre-alarm is initiated and the door is locked open. You enter a code at the keypad to bypass the controller, allowing the elevator car to operate normally. The keypad also provides audible and visual indications of alarms as well as standby, bypass, and power-on conditions.</p>
24 VDC Converter 	<p>Used to power the RS-485 repeater. Must be plugged into an unswitched 120V AC source.</p>


I/O-8 Interface Module

Component	Description
I/O-8 Module 	<p>The I/O-8 Module, used in conjunction with networked Xmark systems, provides interface capabilities for a variety of peripheral devices. Each of the 8 ports can be programmed to function as either input or output, providing easy expansion capabilities without sacrificing space or increasing cost.</p> <p>The I/O-8 Module allows your resident/asset protection system to also operate as a perimeter security system. For example, a networked Xmark system can monitor dry contact or voltage changes if the signal is connected to an input on the I/O-8 Module. Software not only allows Controllers and supervised Inputs/Outputs to be grouped into zones, but also provides timer functionality.</p>


Wiegand Interface

Component	Description
Weigand Interface Module	
	<p>The Weigand Interface allows for simple yet secure bypass of doors and elevators and eliminates the need for the staff member to carry a separate access card while remembering a PIN code for access to the same door. The interface makes it possible to connect industry-standard staff card readers to the RoamAlert system as a means of bypassing protected exit points and elevators. The unit accepts standard 26-bit and other larger capacity Wiegand data formats.</p> <p>The interface converts the Wiegand signal containing the access card ID and sends it to the R3 Controller. The Controller treats the Wiegand signal the same way it treats a Mode 1 Access Keypad signal. This provides an easy and non-intrusive way of interfacing third party card access equipment to Xmark systems for the purposes of entering bypass/reset codes. The Weigand interface has been designed and tested to work with HID Corporation proximity card readers (EntryProx, Thinline II, and other families), but can be used with any other equipment that generates Wiegand output in the same format.</p>

Network Manager (NM)

Component	Description
Network Manager	
	<p>The Network Manager (NM) allows the connection of the RoamAlert RF infrastructure to an existing Ethernet network, thereby simplifying cabling. The NM also allows different applications to simultaneously access the same RF infrastructure devices. To ensure that application software is isolated from network complexity, a communication module is built into the NM. The NM is compatible with Xmark's RoamAlert and Asstrac application software as well as third-party applications connected to the NM through a standard DLL interface. The NM continues to manage the network when an application is disconnected. All events are logged for up to 8-10 hours (under maximum network load) and then passed to the application when it is reconnected.</p>

Remote Display Unit (RDU)

Component	Description
Remote Display Unit	
	<p>The Remote display Unit (RDU) can be mounted near exits or other locations where a console is not practical or necessary. The RDU displays system-wide and local alarms. Users can accept alarms at the RDU without needing to return to a console or the server, a feature useful in large or multi-floor facilities.</p> <p>If located near and connected to a door controller, the RDU can be used as a keypad, as well as for remote alarm clearing. The RDU can be set for HIPAA compliance when you are configuring it in the RoamAlert software.</p>

SYSTEM DESIGN

This chapter discusses:

- theory of operation,
- the system design process,
- assessing the facility,
- planning the location of controller systems,
- creating a receiver coverage plan, and
- designing network and power distribution.

Important: *Carefully plan the location of devices and equipment prior to installing the RoamAlert system. Failure to thoroughly consider in advance all aspects of system design can mean many frustrating hours adjusting the location of devices or re-laying the network or power cabling.*

This chapter provides guidance and instruction in the design of a system. Installation of each device is covered in subsequent chapters.

A minimum system configuration consists of:

- a RoamAlert server,
- door controllers with exciters and optional access keypads,
- elevator controllers in a facility with elevators,
- receivers,
- tag readers, and
- RoamAlert wrist tags.

A RoamAlert system may also include:

- RoamAlert consoles or RDUs (Remote Display Units),
- I/O-8 interface modules,
- Tag Links,
- Wiegand interfaces,
- Paging interfaces, and
- Network Managers (NM).

Theory of Operation

The RoamAlert wander prevention system uses radio frequency (RF) waves to communicate between tags and exciters or receivers, and uses RS485 network cabling to communicate between the RoamAlert server and the system components.

RoamAlert tags are both RF transmitters and receivers. The RoamAlert system uses two different frequencies in two frequency bands, 433.92 MHz in the Very High Frequency (VHF) band and 307 kHz in the Low Frequency (LF) band.

RoamAlert Tag Communications

RoamAlert tags transmit at 433.92 MHz in the VHF band, and receive at 307 kHz. The tag transmissions are picked up by receivers or controllers and relayed to the server.

Exciter Transmissions

RoamAlert tags receive signals from exciters, which transmit at 307 kHz in the LF band. This signal defines the protected area around a door or in an elevator.

About RF Interference

Radio signals can be blocked, distorted, or “drowned out” by other signals. This is a basic fact of all RF communication systems, from remote-control toy cars to satellite phones. You may encounter interference when installing the RoamAlert system. However, the system has been designed to minimize susceptibility to interference, and the right measures can eliminate virtually any difficulties.

There are three kinds of interference that can affect the operation of the RoamAlert system:

- **VHF noise**

VHF noise is generated both by intentional transmitters like communication systems (e.g. paging systems), and by a wide range of electric and electronic equipment. This noise affects the ability of receivers to pick up RoamAlert tag transmissions. In some cases, it may be possible to relocate the interfering equipment. If not, receivers can be positioned so that they are away from these noise sources.

In addition, R3 receivers have an adjustable RSSI (Received Signal Strength Indicator) Threshold that cuts out ambient noise so that tag signals can be clearly picked up. However, the practical result of raising the RSSI on a receiver is that the RoamAlert tag must be closer to the receiver in order for its signals to be detected. In other words, in an RF noisy facility, receivers will have to be installed more closely together to get proper coverage. R4 receivers automatically adjust the RSSI threshold, but the practical result may be the same, that is, receivers may need to be installed more closely together to get proper coverage.

- **LF noise**

LF noise is similar to VHF noise, except that it occurs in the LF band and is usually more localized. LF noise is generated by such electric and electronic equipment as computer monitors and ballasts from fluorescent lights. LF noise can interfere with exciter signals, preventing the RoamAlert tags from picking up these transmissions.

Because LF noise is more localized, it is often easier to eliminate. Noise-emitting equipment may only have to be moved a foot or two to solve the problem. If this is not possible, a slight repositioning of the exciter may be necessary.

- **Physical barriers**

Radio signals do not pass through metal. Wire mesh, foil-backed ceiling tiles, heating and ventilation ducts and other metal barriers in walls and ceilings can block transmissions from the RoamAlert tags and exciters.

Environmental barriers of this kind will be unique to each facility, but are more likely in older facilities. Almost all interference of this type can be overcome with careful design, installation, and commissioning of a RoamAlert system.

System Design Overview

A smooth and successful RoamAlert installation is the direct result of complete system design and planning. Design and installation will include these steps:

Assess the facility carefully. Understand the:

- physical environment,
- radio frequency environment,
- personnel traffic flow,
- exit requirements, and
- usability requirements.

Plan the location of controller systems. Identify:

- all egress points,
- elevator requirements, and
- third-party interfaces (card readers, fire alarm systems, etc.).

Develop a receiver coverage plan. Understand the:

- coverage requirements (e.g., is tag location necessary or not), and
- obstacles to good tag signal reception.

Develop a network cabling and power distribution plan. Identify:

- network layout requirements (run lengths, repeaters, network managers, etc.),
- power requirements (current draws, cable type, plenum conditions, etc.), and
- server and console requirements.

Install the hardware.

- allow sufficient time for each task,
- install all items neatly and mark cables and parts clearly; a careful, easy-to-understand installation will greatly reduce time and effort during troubleshooting and modification,
- coordinate as required with other parties (elevator company, inspectors, etc.), and
- test thoroughly.

Configure and commission the system.

- set up the RoamAlert software (users, tags, nodes, etc.),
- test thoroughly, and
- commission the system.

Assessing the Facility

Each facility is unique, and will present unique installation challenges. The best way to ensure a smooth and trouble-free installation is to perform a comprehensive assessment of the physical environment and the facility's requirements in order to identify potential trouble spots.

Xmark offers a Project Control Worksheet that systematically steps through every aspect of an installation. However, installers may use any system that captures the following essential information. Xmark Technical Service is also ready to assist you with your planning.

Physical Environment

General construction of the facility

Metal significantly impacts radio frequency transmission and reception. Wire mesh and other metal barriers in walls and ceilings can have a major impact on receiver coverage. Facilities with these characteristics will require a denser network of receivers.

Age of the facility

Older facilities, particularly those that have had extensive renovations, are likely to have impediments to RF, e.g. metal in concrete foundation, plaster lath walls, ceiling space restricted with pipes, and heating and ventilation ducts. Tighter receiver spacing will be required. Facilities of more recent construction (within the last 15 years) are likely to have fewer environmental restrictions and receiver coverage may be greater than the average of 20 ft. (6 m) in open areas.

Number of floors to be covered

Multi-floor installations pose the possibility that exciter and receiver coverage could "bleed" from one floor to the next. This is more likely in newer facilities because they are generally cleaner environments. Exciter detection areas will have to be adjusted so that tags on a different floor do not see the exciter. It is also possible in multi-floor installations to have too much receiver coverage. If tag transmissions are being consistently received by too many receivers, there is a risk of saturating the RoamAlert network.

Specific environmental barriers to receiver installation and cable runs

Identify mechanical and electro-mechanical rooms in the protected area, and large metal objects such as pipes and ducts. Receivers should be installed away from these barriers. In addition, ensure cable runs avoid AC power cables, lighting ballast and other noisy locations such as elevator shafts.

Radio Frequency Environment

Other RF communication equipment in use at the facility and any nearby high-powered RF transmitters

There is potential for RF interference in these cases. It is likely that the RSSI threshold (R3 receivers only) will have to be set relatively high to ensure smooth operation. This in turn means that a denser network of receivers will be required.

Types of equipment in use in the planned RoamAlert system area, the floor above, and the floor below

Investigate what computer and medical monitoring equipment is used, where heavy electrical equipment is located, and where potentially noisy AC power cables are run in the ceiling.

Exit Requirements

Identify each exit that will be covered by a controller, and determine the following:

Size and characteristics of the exit

Single door? Double door? Elevator? Emergency exit? Can the exit be covered by a single exciter antenna, or will a second exciter also be required? Is an access keypad required? All these factors affect installation.

Ceiling height and best positioning of the exciter antenna

Identify physical barriers and determine where to place the exciter. If ceilings are much more than 8 ft. (2.4 m), if doors above or below are also protected, or if metal-backed ceiling tiles are in place, the exciter cannot be mounted on the ceiling. Preferred exciter location is beside the door in the wall cavity. (Installation options are shown in the section “Door Controller and Exciter Installation Procedure” on page 3-5)

Physical environment around the door

Avoid installing exciters too close to exit signs, metal door-frames, magnetic locks and public address speakers. Any equipment remaining from an older security system must also be decommissioned and completely removed.

Proximity to other controllers

Will the exciter be within 20 ft. (6 m) of another controller? If a tag can receive communications from two different controllers because of exciter field overlap, the controllers may report the tag communication as noise and fail to generate any alarms. Multiple controllers must be located at least 20 ft. apart to prevent exciter field overlap.

Traffic flows in the area

Is the exit close to where monitored residents are likely to pass? Care will have to be taken to contain the detection area as tightly as possible around the door. In some cases, a passive infrared detector may have to be used in place of door contacts.

Magnetic door lock requirements

Does the facility wish to lock the door when a monitored resident is brought near a closed door? This will require the installation of a magnetic door lock, which generally requires the approval of the local Authority Having Jurisdiction.

Usability Requirements

Number and location of server and consoles

Determine where the RoamAlertRoamAlert server will be located, and the number and location of consoles or RDUs required. Consultation with the client regarding workflow and monitoring station location will help determine console location.

Alarm reporting

Determine how the facility wants to notify staff of alarms. Do they want visual or audible notification? Do they require custom voice alarms?

Testing for RF Noise

The following procedures may be used to test the proposed installation environment. These procedures are performed using the pocket tag reader (**Part # AR3TR01-PRO**). Refer to the Tag Reader User Guide for usage details.

Have on hand detailed scaled floor plans on which to accurately mark noise sources as you perform these tests.

Ambient VHF Noise Testing

This test will assist in determining the amount of ambient VHF noise at 433 MHz in the proposed protected area. High noise levels will require denser receiver spacing to ensure reliable detection of tag signals. Ideally, this test should be performed throughout the protected area.

- Set the pocket tag reader to the **Check 433 MHZ Noise** mode, then move around the protected area and note on the floor plans all locations with significant ambient noise.

Ambient LF Noise Testing

This test will assist in determining the amount of ambient LF noise at 307 KHz. This test should be performed near proposed exciter locations. Since LF noise is very localized, testing will identify noise-producing equipment that may need to be moved away from exciter locations, and will identify areas that should be avoided when tags are bonded or matched.

- Set the pocket tag reader to the **Check 307 KHZ Noise** mode, then, at each exciter location (and, if necessary, each likely bonding location) note on the floor plans all locations with significant ambient noise.

Planning the Location of Controller Systems

Door controllers must be installed at each egress point on the RoamAlert perimeter. A second keypad may be required at exits where residents are regularly moved in and out of the safe area.

In the case where the RoamAlert installation is on a single floor, but an elevator is within the perimeter, there are two alternatives to controlling the elevator itself:

- install a controller outside the elevator, with exciters covering the elevator doors, or
- install controllers at all doors leading to the elevator lobby.

Where the RoamAlert system covers multiple floors, elevator controllers must be installed in each elevator cab inside the RoamAlert perimeter, and each elevator bank must be isolated from the network using an RS-485 repeater. The elevator controller operates on tailored firmware, so it is not interchangeable with door controllers.

Exciter Placement

Placement of the exciter is one of the most important aspects of a successful installation. No tag may be allowed to pass through the exit undetected. Depending on the physical environment at the exit, an exciter detection field can cover an area approximately 20 feet (6m) wide. For a larger exit, or in a poor location, two exciters may be required. In some cases, a final determination can only be made during installation and testing of the controller system.

Figure 2-1 illustrates two typical exciter placement situations. In the upper diagram, the exciter is placed above the door, consequently, the field must be quite large to cover the door completely. This configuration is not suitable for a multi-floor installation where there is door controller on the floor directly above.

In the lower diagram, the exciter is placed in the wall cavity beside the door, thus the field can be made smaller. Although this configuration may be more difficult to install, it is better suited to a multi-floor installation.

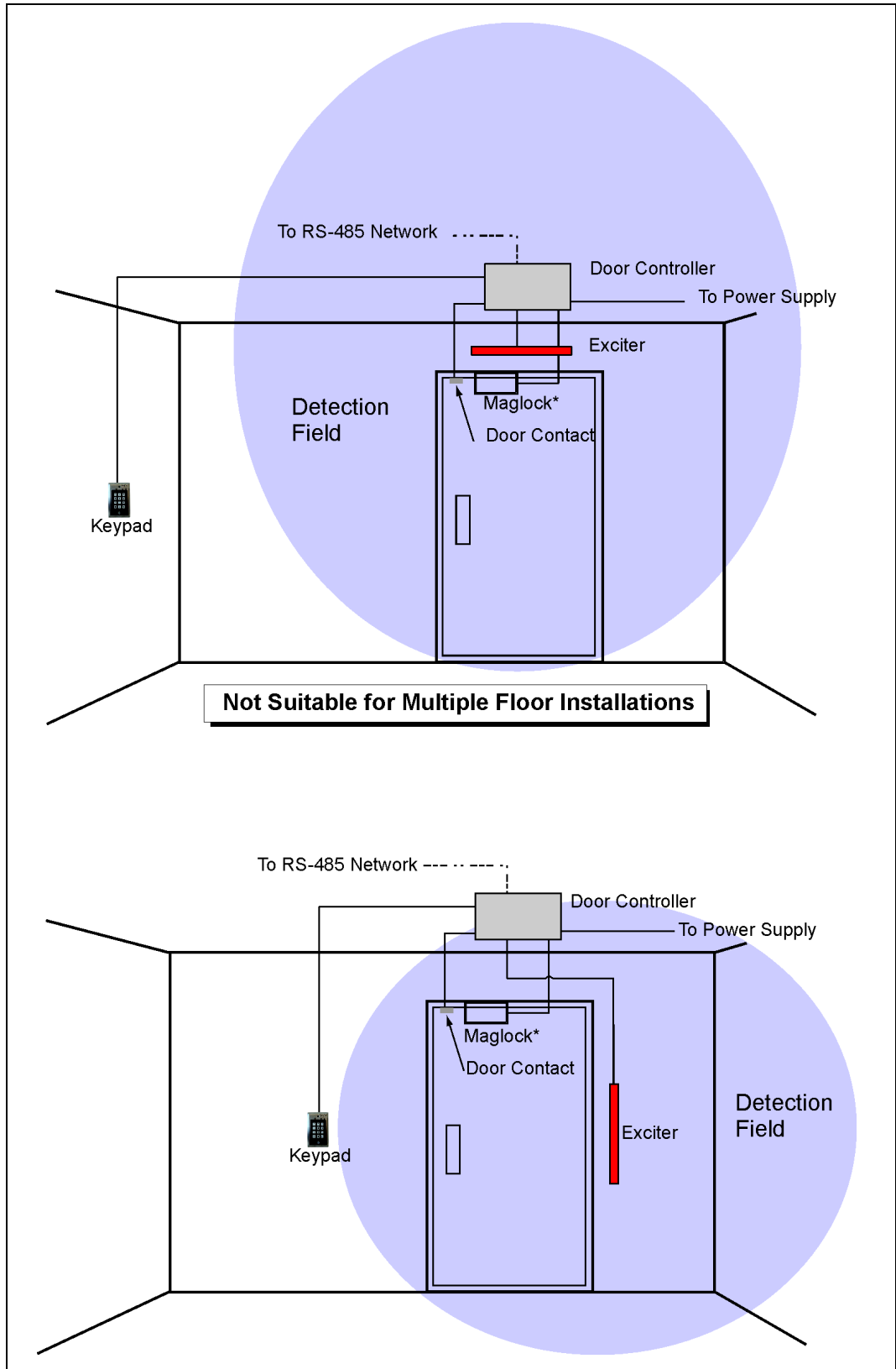


Figure 2-1: Typical Exciter Placement and Coverage

The detection field should not bleed into areas regularly occupied by tags. The detection fields of two controllers in close proximity must not overlap (Figure 2-2). In a multi-floor installation, care must be taken to ensure that the detection field does not overlap fields on the floor above or below (Figure 2-3).

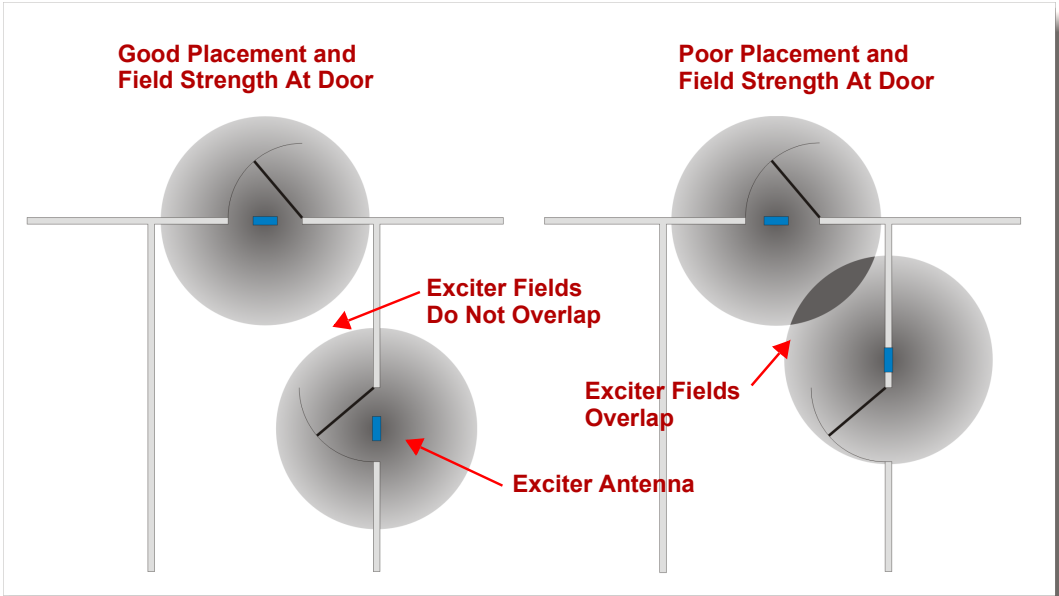


Figure 2-2: Detection Fields in a Multiple Door Installation

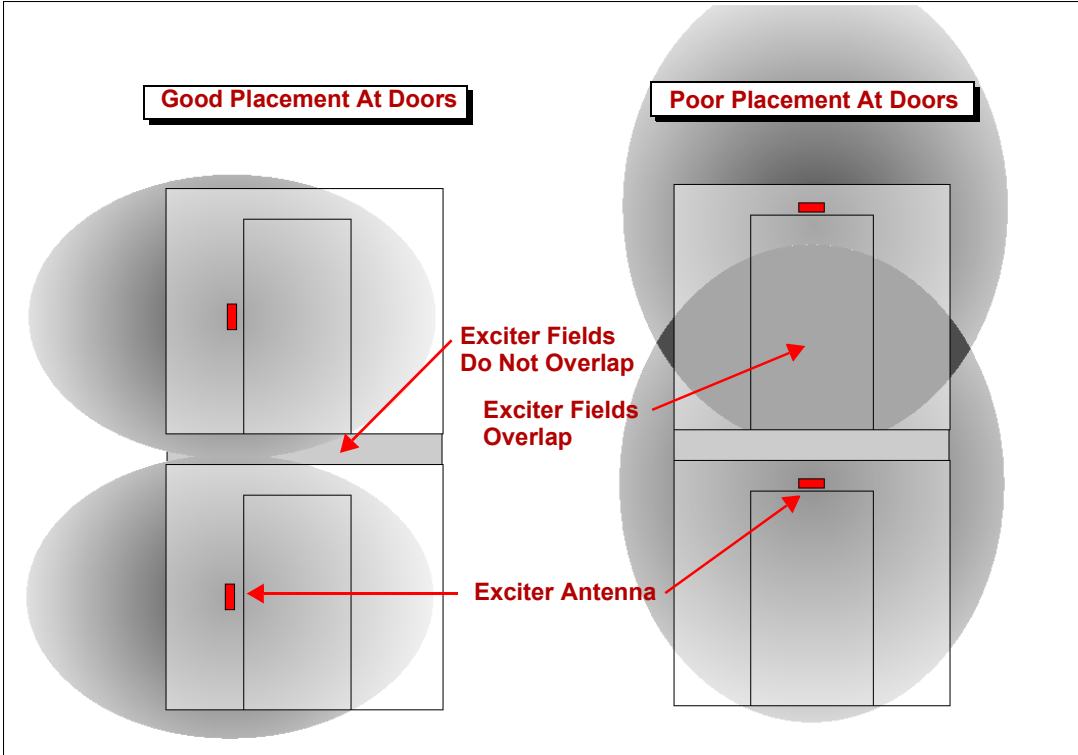


Figure 2-3: Detection Fields in a Multiple Floor Installation

Controller System Layout

Figure 2-4 below shows a schematic overview of the three controller system layouts normally found in a RoamAlert installation: a single door, a double door, and an elevator. Note that a repeater isolates the elevator from the network, the elevator controller is supplied with 120 VAC (usually by the elevator company), and the door controllers are powered by a central power supply.

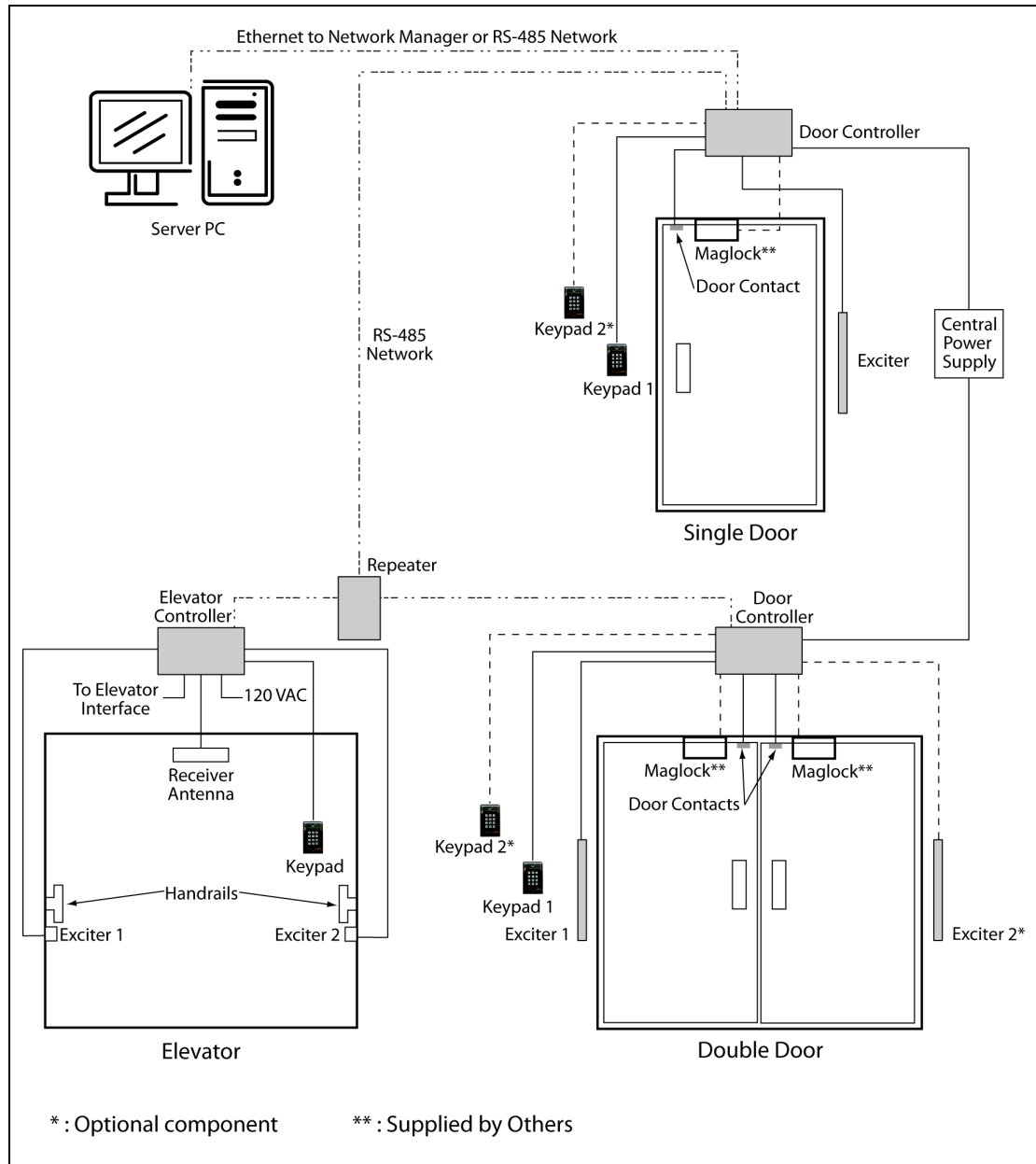


Figure 2-4: Door and Elevator Controller Layout Overview

Creating a Coverage Plan

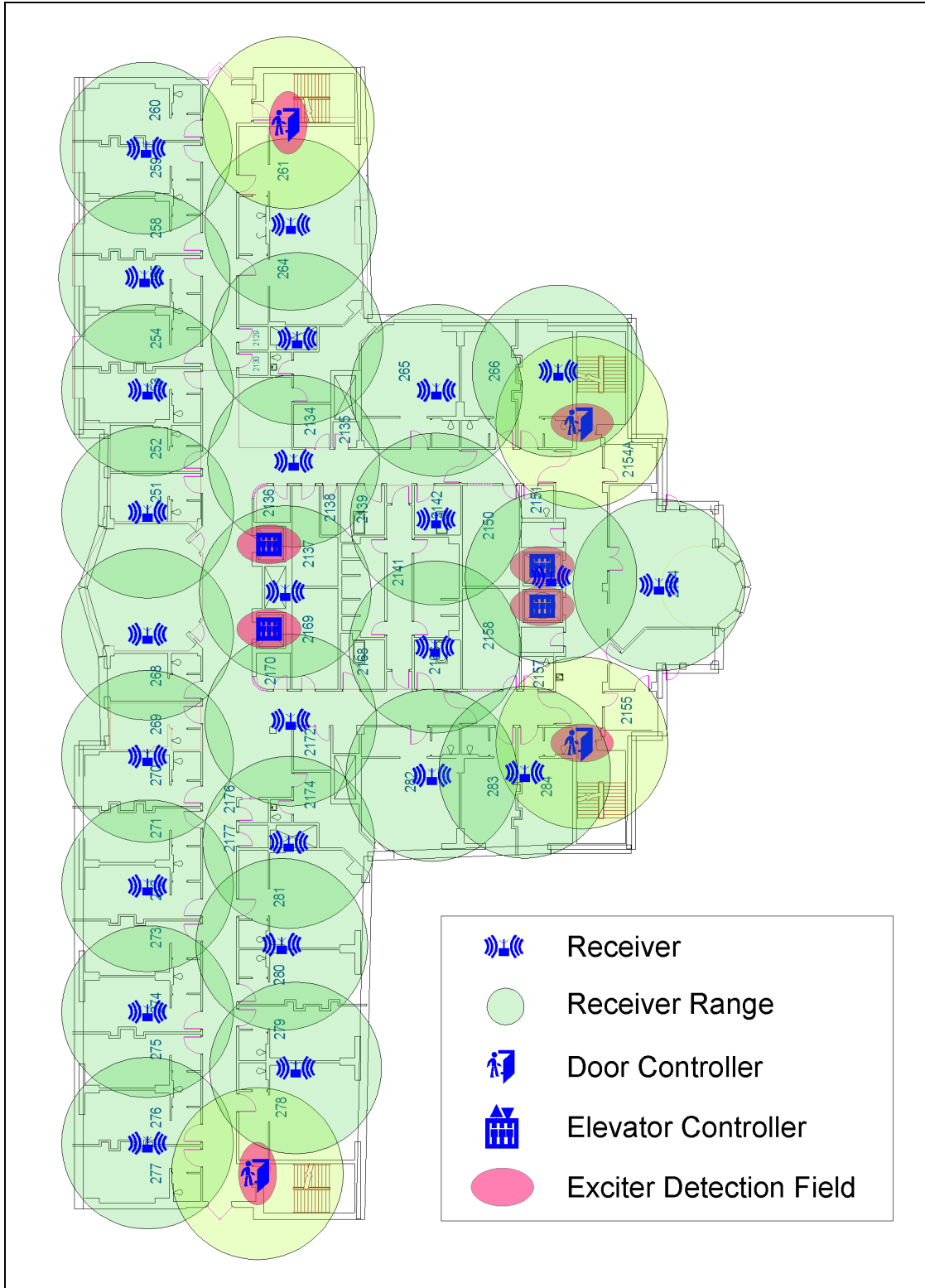


Figure 2-5: Typical Preliminary Coverage Plan

A receiver coverage plan sets out the locations of all receivers within the RoamAlert perimeter. The density of coverage will be determined by several factors, including:

- obstacles in the physical environment,
- level of ambient RF noise, and
- client requirements for duress applications and tag location (denser coverage is necessary for precise location).

You should also identify the locations of controllers, I/O-8 modules and RDUs on the coverage plan. When you install the hardware, you will need to accurately note the controller, receiver, RDU and I/O-8 module serial numbers on the coverage plan. Later, these serial numbers will be entered into the RoamAlert software during the configuration phase (refer to the Software Configuration section for configuration details).

Locating Receivers on the Coverage Plan

As a general rule, a receiver can detect a tag within a 20 ft. (6 m) radius, or approximately 1000-1500 square feet (90-130 square meters). This coverage depends on several factors, including:

- metal barriers between the receiver and tags,
- the presence of wire glass, for example around monitoring stations, and
- walls, equipment and other obstacles.

Note that each door controller includes as part of its circuitry a receiver for the area around the controlled exit.

Materials Required

- Detailed facility assessment. See “Assessing the Facility” on page 2-4.
- Results of RF ambient noise testing. See “Testing for RF Noise” on page 2-6.
- Scaled floor plan (or plans) of the facility, with metal barriers, physical obstructions and noise sources indicated.
- Compass or other device for drawing scaled circles.

Procedure

Using the scaled floor plan as a guide, draw overlapping circles like those shown in Figure 2-5. The center points of the circles indicate the **approximate** location for each receiver.

- 1 Based on the facility assessment and RF ambient noise testing, decide on the radius of the receiver coverage circles for your preliminary design:
 - Few metal barriers or noise sources: suggested radius 20 ft. (6 m)
 - Metal barriers and noise sources: suggested radius 15 ft. (4.5 m)
- 2 Make sure that your floor plan accurately shows all obstructions and noise sources. **Your coverage plan will be flawed if this information is not included.**
- 3 Draw the coverage pattern for all door controllers. Draw a circle with a scaled radius of 15-20 ft. (4.5-6 m) for each door controller.
- 4 Draw the coverage pattern for all corner receivers. Draw circles with a scaled radius of 15-20 ft. (4.5-6 m) in each corner of the protected area, ensuring that the radius intersects the outside corner. This makes sure that receiver coverage will extend right to the corner.
- 5 Draw the coverage patterns for the rest of the facility. Continue to draw overlapping receiver circles, until the entire facility is covered. **Do not place receivers over large metal objects or noise sources.** Shift the receiver to the side, in a location where it can be easily accessed.

- 6 In areas where there are metal obstructions or noise sources, add a receiver to ensure proper coverage. If, for example, there is a wall with wire mesh, add a receiver on the side of the wall with the weakest coverage.

Note:

This is only an approximate indication of where receivers should be located. The procedures in “Installing and Testing Receivers” on page 3-21 may indicate that receivers need to be moved slightly to improve coverage, or that extra receivers are required in certain locations.

Planning the RS-485 Network and Power Distribution

Once the approximate locations of receivers, controllers and I/O-8 modules have been determined, the next step is to design the cabling paths for both network communications and power distribution.

Network Communications

The RoamAlert system is based on the RS-485 network, which is an electrical interface standard for a 2-wire, half-duplex, multi-node bus. The RoamAlert system communicates at 57,600 bps (bits per second) over the network.

Up to 128 nodes (controllers, receivers, I/O-8 modules) can be accommodated on a single network. To extend that limit, or to simplify a multi-floor installation, a network manager (Part # **AR3CT03-000**) may be used.

The RS-485 network has a maximum total run length of 4000 ft. (1220 m) **under ideal conditions**. Actual results vary depending on the number of devices attached, system integrity, ambient influences, and quality of cable. Longer runs require the use of an RS-485 repeater (Part # **AR2NR01-485**) for each additional 4000 ft. of cable. A maximum of 2 repeaters may be used for this purpose.

Repeaters are also used to isolate controlled elevators from the network. Each repeater can connect up to five elevators to the network. A maximum of 5 repeaters may be used for this purpose.

Topology

The network is constructed using a multi-drop BUS topology. Other than the connection of elevator controllers to a repeater, STAR topology must be avoided.

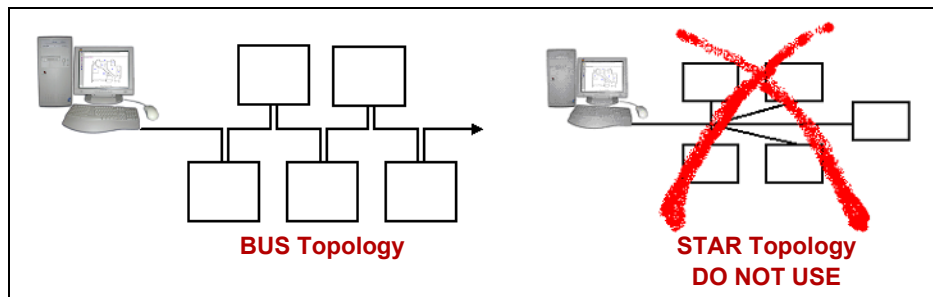


Figure 2-6: Bus vs. Star Network Topology

Network Design Considerations

- Decide in advance where the RoamAlert server and all network devices will be located.
- Route the cable using the shortest possible run length.
- Each segment of the network can accommodate up to 128 devices.
- RS-485 networks must be terminated at the end of the line. Depending on the ending device, a jumper must be set or a 120 Ohm resistor must be added. For example, controllers have on-board termination jumpers, but receivers require the added resistor. The installation chapter of this manual provides details for each network component.
- Conductor characteristics vary with temperature and can degrade substantially outside of their specified range. The RoamAlert system, nevertheless, will function reliably within the 0°C to 50°C range.

- When calculating run lengths and voltage drops, make sure to include at least 10' (3m) of slack for each device.
- Take into consideration the location of panels, conduit, sheet rock and other structural elements that may affect cabling paths.

Good Wiring Practices

The following practises when laying the communication cable will help eliminate problems in device installation and commissioning.

- Label the communication and power cables to distinguish them from other cables.
- Avoid splicing the cable.
- Do not stress the cable or bend it at a sharp angle.
- Where the cable passes over a sharp object, protect it mechanically to prevent damage.
- Keep the cable away from known noise sources, such as fluorescent lights.
- Establish and follow a consistent color-coding system for each wire of the communication and power cables.
- Test the integrity of the communication cable before bringing up the system.

Cable Specifications

The cable types listed below are recommended for the RoamAlert RS-485 network.

Application	Cable Type	AWG	V _{prop} (min.)
Main network segments	twisted pair, solid or stranded core, shielded, 120 Ohms nominal impedance, 15pF/ft maximum nominal capacitance, plenum or non-plenum according to location	24	70
Elevator travelling cable	3 conductor shielded, stranded, low capacitance travel cable	20	N/A

CAT-5 Cable

In general, RS485 is designed for multi-drop, “daisy-chain” operation over a single twisted pair cable with a nominal characteristic impedance of 120 Ohms. This cable is usually 24AWG. Category-5 cable may work in short runs even though its characteristic impedance is 100 Ohms. 32-node RS-485 devices are rated at 100 Ohms, however RoamAlert uses 128-node RS-485 devices rated at 120 Ohms. “Tap points” or “T” connections should be short to eliminate reflections. It is possible to connect several RS485 circuits in parallel if the distances are below about 200 feet per leg @ 9600bps. At greater distances and higher data rates (RoamAlert operates at 57,600bps), the cable impedances add up and load the network. In addition, there is no good way to add termination resistors at the ends of a “Star” network. The combination of the cable impedance and/or termination resistors will load the network and make communications unreliable. Therefore, in order to avoid any communication impairments, we recommend that you use proper RS-485 cable in the correct configuration.

Power Distribution

Power is supplied to all network devices from the Central Power Supply (**Part # AGECP02-024**), a 24 VDC, 10 A power supply, with 8 individual power outputs (1.5 A maximum per output). The power supply requires an input voltage of 115 VAC at 50/60 Hz.

Design Considerations

- Provide power to receivers and controllers from separate outputs.
- No more than 18 receivers per output, to a maximum of 144 receivers per power supply.
- No more than 1 controller per output, to a maximum of 8 controllers per power supply.
- I/O Modules may be powered on the same output as receivers. The voltage for the module is 24 VDC, and it draws a maximum of 800 mA.
- Network repeaters may be powered on the same output as receivers. The voltage for the network repeater is 24 VDC, and it draws a maximum of 100 mA.
- Locate the power supply near an emergency power supply line or other emergency circuit and in a secure location. Where possible, locate the power supply near the center of the network. When more than one power supply is required, aim to distribute them uniformly.
- Observe the run length limitations discussed later in this section, and always test voltage at each device after installation.

The following table shows the power requirements for RoamAlert hardware.

Item	Input Voltage	Current Draw	Remarks
Door Controller	24VDC	1.5A	Based on 300mA for controller, 200mA for the 12V aux. output, and 1.0A for a maglock.
Maglock	12VDC	1.0A	Draws <500mA with a spike when latching
Access Keypad	12VDC	200mA	Powered by the controller
Elevator Controller	110VAC		Separately powered
R4 Receiver	12-24VDC	165mA	125mA pulsed output to drive a relay coil
RS-485 Repeater	9-35VDC		Separately powered
RS-485 to RS-232 Converter	9-35VDC		9VDC power supply shipped with converter
I/O-8 Module	24VDC	800mA	Max. 24VDC @ 100mA per output zone to 500mA total for all output zones
Network Manager	24VDC	500mA	Separately powered
Alarm Output Module	12VDC	1.0A	Separately powered
Wiegand Interface	12VDC	> 50mA	Add card reader current if powered by controller

Figure 2-7: RoamAlert Hardware Power Requirements

Power Cable Run Lengths

The basic formula for calculating power cable run lengths is:

$$\left(\text{Length} = \frac{\text{Voltage Drop} \times \text{Wire Size}}{2 \times \text{Resistivity of Wire} \times \text{Total Device Current}} \right)$$

In this formula, the following assumptions have been made:

- **Voltage Drop** = 12V for a 24V power supply,
- **Wire Size** = 2548 circular mils for 16 gauge wire,
- **2** = the length must be doubled for a complete circuit,
- **Resistivity of Wire** = 12 for copper wire at full capacity, and
- **Total Device Current** = the number of devices times 100mA (0.1) per device.

We can, using these values, derive the following table of worst-case scenarios of a device cluster at the end of a wire run:

# of Devices	Maximum Cable Length per Output	
	Meters	Feet
5	777	2548
10	388	1274
15	259	849
20	194	637
25	155	510

Figure 2-8: Theoretical Run Length Limits

The following table shows the voltage drop over distance where devices are spaced approximately 65 feet (20 metres) apart.

Device #	Current	Distance		V_{DSEG}	V_{DACC}
		Meters	Feet		
0	0	0	0	0.00	0
1	2.5	20	65	1.53	1.53
2	2.4	40	130	1.47	3.00
3	2.3	59	195	1.41	4.41
4	2.2	79	260	1.35	5.76
5	2.1	99	325	1.29	7.04
6	2	119	390	1.22	8.27
7	1.9	139	455	1.16	9.43
8	1.8	158	520	1.10	10.53
9	1.7	178	585	1.04	11.57
10	1.6	198	650	0.98	12.55
11	1.5	218	715	0.92	13.47
12	1.4	238	780	0.86	14.33
13	1.3	258	845	0.80	15.12
14	1.2	277	910	0.73	15.86
15	1.1	297	975	0.67	16.53
16	1	317	1040	0.61	17.14
17	0.9	337	1105	0.55	17.69
18	0.8	357	1170	0.49	18.18
19	0.7	376	1235	0.43	18.61
20	0.6	396	1300	0.37	18.98
21	0.5	416	1365	0.31	19.29
22	0.4	436	1430	0.24	19.53
23	0.3	456	1495	0.18	19.71
24	0.2	475	1560	0.12	19.84
25	0.1	495	1625	0.06	19.90
Notes:	<p>V_{DSEG} = Voltage drop over the individual segment</p> <p>V_{DACC} = Accumulated voltage drop as distance from the power source progresses</p> <ul style="list-style-type: none"> • Devices are spaced 65 ft (20 m) apart. • Each device draws 0.1A. • 16 gauge wire is assumed. • Device voltage is 12V to 24V. • Green rows show acceptable limits, so 585 ft (178 m) is the maximum total run length from the power source (out and back) for this scenario. 				

Figure 2-9: Voltage Drop Over Distance

HARDWARE INSTALLATION

This chapter describes the physical installation and testing of all system components, including:

- power supplies and cabling,
- RS485 network cabling,
- door control systems (controller, exciter, keypad, switch, maglock, Wiegand interface),
- elevator control systems (controller, exciter, keypad, repeater),
- receivers,
- I/O-8 modules,
- Alarm Output modules,
- RDUs (Remote Display Units), and
- Network Managers (NM).

Each component can be physically installed independently of the others, but it is advisable to begin with the power supply, and the power distribution and network cabling, so that power and network connections are available for testing before the location of each device is finalized.

Important: *Before you begin installation, you should have on hand a preliminary coverage plan clearly identifying the location of all door and elevator controllers, receivers, and I/O-8 modules.*

On this plan, record the serial numbers of the nodes as you install them. Later, during software configuration, you will enter the corresponding serial numbers as you add the nodes to the RoamAlert software.

This plan should also accurately show all obstructions and RF noise sources that may affect device placement and cable layout. Development of the plan is discussed in “Creating a Coverage Plan” on page 2-11.

General Installation Tips

Keeping these tips in mind as you work will help you to complete an installation that makes effective use of your time, minimizes mistakes, reduces testing time, prepares for easy maintenance and upgrades, and produces a clean and professional system.

- **Have all your equipment and plans on hand.**
Know the requirements for the installation of each device before you begin. Make sure to have complete coverage and device location plans ready.
- **Complete all commissioning forms.**
A little extra time spent documenting the system as you install it will save a great deal of time later when performing maintenance or upgrades. Record all serial #'s on your as-built drawings, and ensure that all device settings are recorded on the commissioning forms.
- **Provide adequate cable support.**
Do not rely on cable connectors or terminal strips for cable support – use cable clamps and cable ties to provide strain relief.
- **Clearly label all cables.**
Marking cables during installation will help to ensure that connections at each end are correct, and will ease maintenance and troubleshooting later.
- **Route cable carefully and provide adequate slack.**
Avoid metal barriers, heat sources, and other obstructions. Do not bend cable sharply or allow kinks to develop. Leave a minimum of 10' (3 metres) of slack to accommodate adjustments in device location. Do not forget to include the slack in run length calculations.
- **Install exposed devices neatly.**
A professional, clean-looking and tidy installation is one of the best marketing tools you can have for your services.
- **Do not mount devices permanently until testing is complete.**
For door controllers, make sure to test door lock response and tag detection. For receivers, make sure the entire site is tested. Sites that use TLM (Tag Location Monitoring) will require more receivers for adequate coverage.
- **Back up your power systems with UPS (uninterruptable power supply).**
All Xmark equipment should be deployed on a UPS-backed power system. Hospital emergency power generators can have up to seven second time lapses which can cause software and hardware problems.
- **Do not skimp on the quality or quantity of materials.**
For example, using the appropriate communications cable for the specific application (RS-485 runs, elevator traveling cable, etc.) will prevent future problems that may impair operation. Use appropriate numbers of power supplies, repeaters and receivers for the application.

Installing Power, Wiring and Network Cabling

The installation of central power supplies will depend on a variety of factors, such as:

- the availability of suitable locations for the power supplies themselves,
- the number of devices being installed in the system,
- the locations of these devices: e.g., multiple floors or buildings, and
- the physical environment.

Installing the Central Power Supply and Wiring

Xmark recommends that all RoamAlert devices be powered by UPS-backed central power supplies. This will serve to isolate the RoamAlert system from the vagaries of the facility's general power network, and will ensure that RoamAlert will continue to operate for a period of time during power outages. Note that facility back-up power generators can have delays of several seconds before coming online. During this period, damage can be done to the RoamAlert system.

The exception to this rule is the elevator controller and associated repeaters, which should have unswitched 120 VAC service in close proximity. Refer to "Installing and Tuning Elevator Control Systems" on page 3-25 for details.

Installation Tips

- **Carefully calculate all loads and power requirements.**
This exercise will help you to identify the number and configuration of power supplies required for the installation.
- **Select location(s) based on security needs and convenience.**
Power supplies should be located so that tampering is discouraged and so that wiring and maintenance are simplified.

Installation Procedures

Important: *Refer to the manufacturer's documentation for central power supply installation procedures.*

Installing the RS-485 Network Cabling

Determine the locations of the RoamAlert server, door and elevator controllers, receivers, I/O-8 modules, repeaters and, if you are using them, network managers.

Installation Tips

- **Calculate all run lengths carefully.**
Theoretically, an RS-485 segment can be up to 4,000 feet in length under ideal conditions. However, as you add devices and take environmental factors into consideration, the feasible length will be much shorter. Include about 10 ft (3 m) of slack for each device to account for adjustments in location.
- **Route cables carefully.**
Do not allow kinks to develop, do not make sharp turns, and avoid sources of interference such as power cables, fluorescent lighting, etc.

Installing and Testing the Door Control System

A door control system includes the following minimum components:

- one R3 controller,
- one SRA exciter antenna with 25' co-axial cable,
- one receive antenna,
- one access keypad, and
- one magnetic door switch (two supplied).

Depending on the physical environment or client requirements, you may also be installing:

- a second exciter,
- a second door switch,
- one or two maglocks,
- a second keypads, or
- one Wiegand interface.

You may also be connecting the door controller to fire alarm systems, nurse call system annunciators or other equipment.

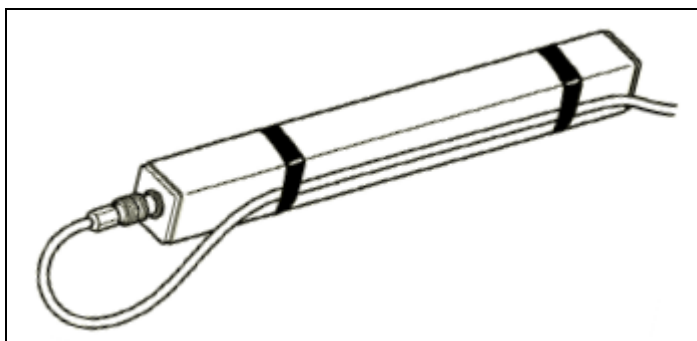
Door Controller Installation Tips

- **Run network and power cables to each controller location prior to installation.**
Leave at least 10 ft. (3 m) of slack, as adjusting the controller's location may be required to optimize receive antenna reception.
- **Mount the controller with sufficient clearances. You must be able to:**
 - access the front panel connectors,
 - open the hinged top to make switch and jumper adjustments, and
 - position the receive antenna vertically. If this proves to be impossible, you can use an elevator receive antenna (**Part # AR2RA01-L00**).
- **The receive antenna must have a clear receive path.**
Ensure that the controller's receive antenna is not obstructed by metal influences such as bulkheads, ductwork, metal panels, and the like. The antenna must have a clear receive path from all potential tag transmission positions.
- **Mount keypads permanently after the exciter detection field has been finalized.**
Keypads should be mounted outside the exciter detection field for staff convenience.
- **Document the installed controller.**
For each door controller installed, print and complete **Form 16**. Include this form in the System Commissioning binder.

Exciter Installation Tips

- **The exciter may be placed in a number of positions, depending on the environment:**
 - above the doorway, laid flat on the dropped ceiling tile (non foil-backed),
 - inside a wall cavity, four (4) feet above the floor,
 - on the sidewall along the hallway, four (4) feet above the floor,

- securely fastened under the floor of the doorway, or
- placed on an exterior wall to limit penetration of the field into the building.
- **The exciter field must not extend into areas that are regularly occupied by tags.**
These tags could keep a controller in the pre-alarm state, preventing the door from opening if maglocks are in use.
- **Tags should detect the exciter field at least six (6) feet from the door to allow sufficient time for a maglock to energize.**
- **If the exciter is being dropped inside a wall cavity:**
 - To prevent damage to the connector, do not let the exciter hang by the cable. Loop the cable and wrap it with a tie-wrap or a band of electrical tape, as shown here:



- do not let the exciter hang so low that it touches the bottom steel plate, and
- mark the correct height on the cable before dropping the exciter into the cavity, then secure the cable when it is hanging in position.

Receive Antenna Installation Tips

- **Position the antenna in a vertical orientation.**
The antenna includes a removable right angle fitting to aid in positioning.
- **The antenna has a maximum receive range of 30 feet (9 meters).**
- **There must be no metal barriers blocking tag signals.**
The receive antenna should be positioned below metal pans, foil-backed ceiling tiles, etc. If this is not possible, you may substitute an elevator receive antenna to aid in positioning.

Door Controller and Exciter Installation Procedure

Follow these steps to install and test the controller, exciter and receive antenna.

- 1** Record the controller's serial number on the facility floor plan at the correct location. This serial number is required during software configuration to identify the controller. The serial number is found on the back of the controller beneath the bar code.
- 2** Place the controller at the approximate final location.
- 3** Set the controller mode switch, **SW102**, to **Position 0** (test mode). **SW102** is beige and located in the upper right quadrant of the controller circuit board. **Do not forget to reset this switch when installation is complete.**
- 4** Set the receiver threshold switch, **SW201**, to position 4 (medium sensitivity). **SW201** is beige and located at the lower left of the controller circuit board.

- 5 Connect the receive antenna to the **Receive Antenna** BNC terminal on the controller front panel. Orient the antenna vertically for best reception. If necessary, you can loosen the whip with an Allen key and locate it at the end of the BNC connector.
 - 6 Connect one end of the exciter cable to BNC terminal **SRA #1** on the controller front panel, and the other end to the BNC terminal on the exciter. If you are installing two exciters, connect the second cable to **SRA #2** and the second exciter.
 - 7 Connect an access keypad to the **Keypad** terminal on the controller front panel using the supplied cable. The keypad is used later in this procedure during exciter setup for audible confirmation of tag in field. See “Installing a Keypad” on page 3-15 for permanent keypad installation steps.
 - 8 Connect the power cable to lines 1 (**+24V DC Input**) and 2 (**System Ground**) on the controller terminal block.
 - 9 Position the exciter at the location where you estimate that the best field will occur. **The field must fill the area in front of the door all the way to the floor so that no tag can reach the door undetected.** To tune the exciter field:
 - 9.1 Apply power to the controller.
 - 9.2 Place a test tag on a non-metallic surface, about four (4) feet above the floor, at the maximum distance (not more than 10 feet) from which you have determined that the tag should be detected.
 - 9.3 Using switch R520 (the large blue potentiometer at the upper right of the controller circuit board), adjust the range of the exciter field. Turn the pot clockwise to increase the field range, counter-clockwise to decrease it. Decrease the field until the tag is no longer detected, then increase the field until the tag is reliably detected.
 - 9.4 Pick up the test tag and slowly pass it through all the areas that you need the field to cover (**do not forget the floor**). The keypad should beep at a steady rate. An uneven rate indicates that the exciter field is poor at that location.
 - 9.5 Finally, take the test tag into any adjacent rooms or areas that may be regularly occupied by tags. If the tag is still detected, the exciter field will need to be decreased.
- Important:** 10 Reset the controller mode switch, **SW102**, to one of its non-test positions (see Table 3.3 for settings).

Controller Connection Notes and Diagrams

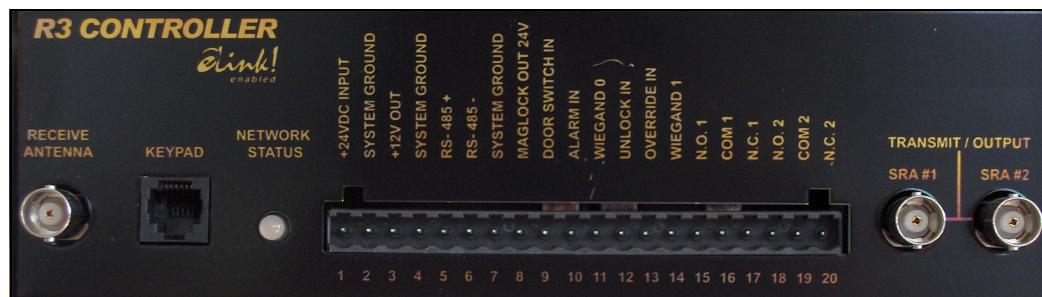


Figure 3-1: R3 Controller Front Panel Connectors

Table 3.1 R3 Controller Front Panel Connectors – Left to Right

#	Name	Remarks
–	Receive Antenna	BNC connector for whip or elevator-style cable antenna. Do not exceed 3 feet of RG58/U antenna cable.
–	Keypad	RJ-11 connector for keypad. Two keypads can be connected using a modular Y adapter (Part # AR3KA01-001)
1	+24VDC INPUT	Powers the controller (250 mA), maglock (1.0A max), and +12 VDC auxiliary output (200 mA max).
2	SYSTEM GROUND	Common Ground
3	+12V OUT	Power for ID display, select sound, etc.: 12VDC, 200mA max
4	SYSTEM GROUND	Common Ground for 12VDC auxiliary power output
5	RS-485 +	Network connectors to the next and previous devices on the RS-485 bus. If this is the last device on the bus, make sure to set jumper JP401 ON. (120 Ohm termination resistor)
6	RS-485 -	
7	SYSTEM GROUND	Ground for RS-485 and MAGLOCK OUT 24V. Select one device only for RS-485 ground.
8	MAGLOCK OUT 24V	Power (24 VDC, 1.0A max) to energize a magnetic door lock while a Tag is in the detection zone.
9	DOOR SWITCH IN	Active low signal (ground), activates the alarm relays and keypad alarm indicators while the door is open and a Tag is in the detection zone. Connect double door switches in series so that opening either door activates the alarm.
10	ALARM IN	Activates the maglock, alarm relays, and keypad alarm indicators when connected to system ground, even if no Tag is in the detection zone.
11	WIEGAND 0	Not used
12	UNLOCK IN	Deactivates the maglock when connected to system ground. Typically connected to fire alarm panel auxiliary trouble relay to unlock the door if a fire is detected. Also deactivates alarm relays and keypad alarm indicators.
13	OVERRIDE IN	Deactivates the maglock, alarm relays, and keypad alarm indicators when connected to system ground, even if the door is open and a Tag is in the detection zone.
14	WIEGAND 1	Not used
15	N.O. 1	Alarm Relays 1 and 2 are activated when the door is open and a Tag is in the detection zone or when ALARM IN is connected to system ground. Alarm Relays 1 and 2 are deactivated when the alarm is cleared (see Mode Switch description in Table 3.3 below) or OVERRIDE IN or UNLOCK IN is connected to system ground. Maximum relay contact current is 2A @ 30 VDC.
16	COM 1	
17	N.C. 1	
18	N.O. 2	
19	COM 2	
20	N.C. 2	
–	SRA #1	BNC connectors for two exciter antennas. Do not exceed 25 feet of RG48 cable for each antenna. Do not terminate unused connector.
–	SRA #2	

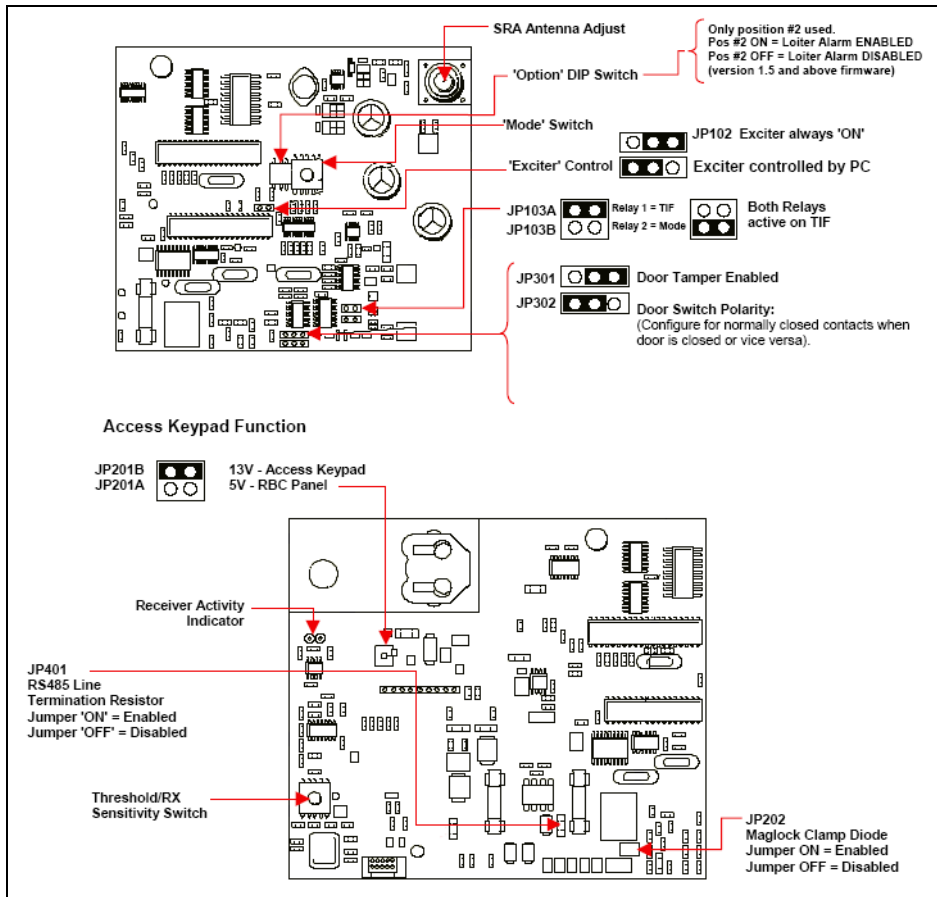


Figure 3-2: R3 Controller Jumpers and Switches

Table 3.2 R3 Controller Jumpers and Switches

Label	Default	Description	Remarks
JP102	Pos 1-2	Pos 1-2 – Exciter always on Pos 2-3 – Exciter controlled by PC	Do not change default setting.
JP103A JP103B	Pos A	Pos A – Relay 1 = TIF, Relay 2 = Mode Pos B – Both relays active on TIF	
JP201A JP201B	Pos B	Pos B – 13V - Access Keypad Pos A – 5V - RBC Panel	
JP202	ON	ON – Maglock Clamp Diode Enabled. Prevents relay contact damage caused by inductive kickback from the maglock. Will override the fast release of maglocks with that feature. OFF – Maglock Clamp Diode Disabled. For maglocks with a fast release feature.	Set this jumper OFF if the installed maglock has fast release and you want to preserve that feature.
JP301	Pos 2-3	Pos 2-3 – Door Tamper Disabled Pos 1-2 – Door Tamper Enabled	Do not change default setting unless you supply a supervised door switch.
JP302	Pos 2-3	Pos 2-3 – Meant for contacts that are closed when the door is closed . Pos 1-2 – Meant for contacts that are closed when the door is open .	
JP401	OFF	OFF – RS-485 line termination resistor disabled ON – RS-485 line termination resistor enabled	Set to ON only if this is the last device on the RS-485 bus.
LD501	N/A	Receive indicator: lights momentarily each time a tag is detected. Flickers continuously if random RF noise signal is received.	Located at the upper left of the board, used for testing receive antenna reception during installation.
SW102	Pos 3	Controller mode switch: Pos 3 = Unlatched – alarm automatically terminates	See Table 3.3 for mode switch settings.
SW103	SW 2 ON	SW 2 ON – Loiter alarm enabled SW 2 OFF – Loiter alarm disabled	SW 1 is not used.
SW201	Pos 4	Receiver threshold switch: adjust for optimum noise suppression and tag reception. 0 = OFF, receiver disabled 1 = low sensitivity, high noise suppression 7 = high sensitivity, low noise suppression 8, 9 = highest sensitivity, no noise suppression	
R520	N/A	Exciter antenna adjust: controls the power of the exciter field. Turn clockwise to increase the field power and detection zone size.	Do not set a detection zone larger than 10 feet.
Network Status (on front panel)		OFF – no power to controller. Solid green – Normal operation and RS-485 network communication. Solid red – RS-485 network communication never established. Flashing red/green – RS-485 network communication established, then lost.	

Table 3.3 R3 Controller Mode Switch (SW102) Settings and Relay Action

Position	Description	Relay Action	
		Relay 1	Relay 2
0	Test mode. Use only while testing during installation or troubleshooting.	No action	No action
1	Non-latched alarm – automatically terminates	Active TIF D/O	Active TIF D/O or D/C
2	Latched alarm – does not terminate	Active TIF D/O	Active TIF D/O or D/C
3	Non-latched alarm – automatically terminates	Active TIF D/O	TIC
4	Latched alarm and pre-alarm	Active TIF D/O	TIC
5	Non-latched alarm – automatically terminates	Active TIF D/O	Active on Bypass
6-9, A-F	Not used.		
		D/O = Door Open, D/C = Door Closed TIF = Tag In Field (in exciter detection zone) TIC = Tag Initiated Communication (tamper)	

Connecting a Third-Party Keypad

Third-party keypads can be connected to an R3 controller using a **6P6C** modular plug according to the following pin-outs at the controller keypad jack, from left (pin 1) to right (pin 6):

Pin	Description
1	+12V DC
2	Ground
3	BYPASS_IN
4	RESET_IN
5	ALARM_OUT
6	BYPASS_OUT

Installing a Magnetic Door Switch

The door switch supplied with the controller kit is a two-part magnetic switch. The magnet is attached to the door and the switch is attached to the door frame (with the supplied cover plate). The switch has three connectors: NO (Normally Open), NC (Normally Closed) and COM (Common Ground). When the door is open (switch not magnetized), NC is connected. When the door is closed (switch magnetized), NO is connected. See Figure 3-5 on page 3-12 for the wiring diagram.

Using a Supervised Door Switch

In some installations, you may wish to know when the door switch has been tampered with, i.e., if the switch has been hard-wired or open-circuited. In such cases, you will need to supply a supervised door switch with 1 K resistors and set jumper JP-301 on the door controller to Door Tamper Enabled (pins 1 and 2 jumpered). Alternately, you can wire the supplied door switch with two 1 K resistors that create a “potential divider” as the basis for tamper detection.

Door Switch Installation Tips

- **Ensure the correct orientation and position of the parts.**
When correctly installed, and the door is closed, the arrow on the switch face aligns with the arrow on the magnet face and the gap between switch and magnet does not exceed 5/8”.
- **Ensure that jumper settings and connections are consistent.**
If jumper JP-302 on the controller is set to normally closed (pins 2 and 3 jumpered), connect NO on the switch to DOOR SWITCH IN on the controller.
- **Don’t forget the cover plate.**
When attaching the switch, position the cover plate over the terminals after connecting the wiring and before screwing the switch to the door frame.
- **Wire two door switches in series.**
For double doors, two door switches are required. They must be wired in series rather than parallel. See Figure 3-5 on page 3-12 for the wiring diagram.

Door Switch Installation Procedure

Follow these steps to install and test a single door switch for a default situation.

- 1 Ensure pins 2 and 3 (door tamper disabled) are jumpered on **JP-301** on the controller.
- 2 Ensure pins 2 and 3 (door switch NO connected) are jumpered on **JP-302** on the controller.
- 3 Prepare the door frame for attachment of the switch and routing of the wiring (see Figure 3-4 on page 3-12 for switch and hole placement dimensions and clearances).
- 4 Route the supplied cable from the controller to the switch.
- 5 Connect **NO** on the switch to **DOOR SWITCH IN** (Pin 9) on the controller front panel.
- 6 Connect **COM** on the switch to **SYSTEM GROUND** (Pin 7) on the controller front panel.
- 7 Attach the switch to the door frame. Don’t forget the cover plate.
- 8 Attach the magnet to the door, making sure to align the arrow on the magnet with the arrow on the switch (see Figure 3-4 on page 3-12 for switch and hole placement dimensions and clearances and Figure 3-3 for location of alignment arrows).
- 9 To test the switch:

- 9.1 Do NOT power up the controller.
- 9.2 Connect a continuity tester to **DOOR SWITCH IN** (Pin 9) and **SYSTEM GROUND** (Pin 7) on the controller front panel.
- 9.3 Close the door. The tester must read a closed circuit when the door is closed.

Door Switch Notes and Diagrams



Figure 3-3: Door Switch Showing Alignment Arrows

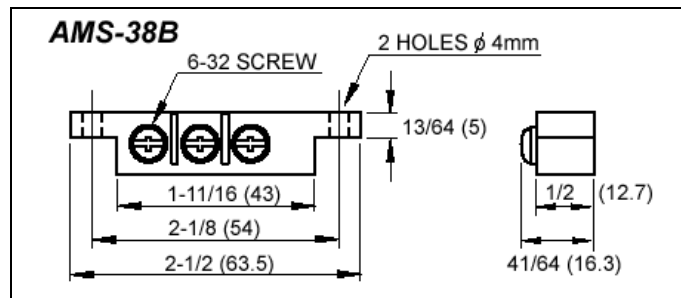


Figure 3-4: Door Switch Dimensions and Clearances

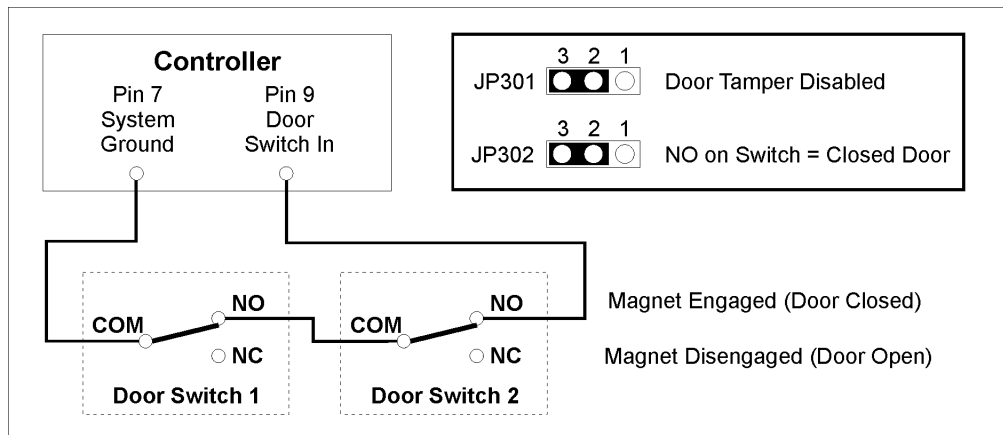


Figure 3-5: Door Switch Wiring Diagram

Installing a Maglock

The R3 door controller has two connectors on the front panel and a jumper on the circuit board that work together to control a maglock.

- **MAGLOCK OUT 24V** (Pin 8) provides 1 Amp of power to the connected maglock when a TIF (Tag In Field) is detected.
- **UNLOCK IN** (Pin 12) disables MAGLOCK OUT 24V when it receives an active low signal from an external source such as a fire alarm system or sprinkler system.
- **JP202** enables or disables a 3A clamp diode built into the controller circuitry. If the maglock you are installing presents an inductive load to the controller, set the jumper on JP202.

Important: **UNLOCK IN** must be connected to the appropriate interface signal of the external system to ensure that the maglock is defeated when the system is activated. The input must remain active low until manually reset at the external system, so that the maglock does not re-engage. For example, a fire alarm system would be connected to **UNLOCK IN**.

Important: The system grounds on the controller are connected to the controller's metal housing. In a RoamAlert system powered by a central power supply, all DC returns (**SYSTEM GROUND**, Pin 2 on the controller) must be returned to the CPS Common Ground. We recommend that each controller be connected to the CPS through a UL approved 1.6A time delay fuse.

Maglock Installation Tips

- **Maglock used cannot exceed 1 Amp of power and must be rated at 24V.**
The average maglock draws up to 400mA, depending on the size. A dual maglock (for double doors) will have a higher consumption. A 24VDC form "C" relay can be used to energize multiple maglocks or maglocks that draw more than 1 Amp. An external power supply can be connected to the contact side and the controller maglock output to the coil to activate the relay.
- **Ensure proper interface to fire alarm or sprinkler systems.**
The maglock must be defeated in fire or other emergency situations. Contact the appropriate local authorities if necessary.
- **Maglocks must be wired in parallel for double door installations.**
If you use two maglocks for a double door installation, ensure that they are wired in parallel to **MAGLOCK OUT 24V** and **SYSTEM GROUND** so that they both engage in an alarm condition. The momentary current draw during latching may slightly exceed 1Amp. This should not cause any problems. Alternately, you can install a double-coil (double-gang) maglock designed specifically for double doors.
- **Using delayed egress maglocks.**
Delayed egress maglocks are often specified by authorities. These maglocks are best configured to energize when power is applied, so that **MAGLOCK OUT 24V** can still be used. If, however, the release terminals of the maglock must be used, one of the auxiliary relays of the controller has to be used for maglock operation.

Maglock Installation Procedure

Follow these steps to install and test a maglock:

- 1 Follow manufacturer's instructions for physical installation of the maglock.
- 2 Set the jumper on **JP202** on the controller circuit board to enable the controller's 3A clamp diode only if the maglock presents an inductive load (see manufacturer's documentation).

- 3** Connect the external fire alarm or sprinkler system input to **UNLOCK IN** (Pin 12) on the controller front panel.
- 4** Connect the 24V power wire from the maglock to **MAGLOCK OUT 24V** (Pin 8) on the door controller front panel.
- 5** Connect the ground wire from the maglock to **SYSTEM GROUND** (Pin 7) on the door controller front panel.
- 6** To test the maglock:
 - 6.1** Supply power to the controller and close the door.
 - 6.2** Bring a tag into the exciter field and ensure that the maglock engages.
 - 6.3** While the maglock is engaged, provide an active low signal through **UNLOCK IN** and ensure that the maglock releases.

Installing a Keypad

The access keypad is used by facility staff to temporarily bypass a protected exit, allowing a tag to enter the exciter field without generating an alarm. The keypad also produces audible and visual indication of alarm and bypass conditions and visual indication of power on.

When the door controller is placed in test mode (Position 0, SW102), the keypad can be used to help tune the exciter field (see “Door Controller and Exciter Installation Procedure” on page 3-5).

Two installation modes are available (set by JP3 on the back of the keypad):

- **Mode 1 (formerly known as PINpad mode).**
Up to 1000 unique PIN (Personal Identification Number) codes can be stored in the door controller and managed at the RoamAlert server PC. In this mode, the RoamAlert software tracks each code in the Activity Log. Use this mode when the facility requires a record of which staff member bypassed the exit at a specific date and time.
- **Mode 2 (formerly DKY Keypad mode).**
This mode uses four generic passcodes, 2 for bypass and 2 for reset. Mode 2 is much easier for the facility to administer, but it does not provide the detailed tracking and added security of Mode 1. In Mode 2, only the date and time of each bypass is recorded in the Activity Log.

Keypad Installation Tips

- **Select the appropriate mode for this installation.**
Identify whether the facility requires unique PIN codes or not.
- **Select the appropriate volume level for audible alarm indication.**
Is the keypad located in an area that must be kept quiet? The keypad has 5 volume levels plus inaudible (off). Select the level according to facility requirements.
- **Decide whether the keypad should initiate bypass prior to or after tag detection.**
Mount the keypad outside the exciter field to allow bypass before tag detection.
- **Use the Y adapter for dual keypad installations.**
If the exit requires two keypads (one on each side of the door), use the supplied Y splitter to connect both keypads to the jack on the front of the controller.

Keypad Installation Procedure

Follow these steps to install a keypad:

- 1** Place the jumper on the upper 2 pins of **JP3** on the keypad back to select Mode 1 (unique PIN codes) or place the jumper on the lower two pins to select Mode 2 (generic codes). If this is to be a Mode 2 keypad, continue with “Mode 2 Passcode Programming Procedure” on page 3-16 after completing keypad installation. See Figure 3-6 on page 3-17.
- 2** Set the appropriate volume level on **J1** on the keypad back. Place the jumper on the top pair of pins to set the volume to inaudible (off). Each lower pair of pins increases the volume, with the bottom pair being the loudest. See Figure 3-6 on page 3-17.
- 3** Mount a standard single-gang electrical box (not supplied), or the supplied low-voltage retrofit bracket, at a convenient height (usually wall switch height) in the selected location (usually just outside the exciter field). Careful placement (not crooked) of all exposed components is the hallmark of a professional installation.
- 4** Run the supplied keypad cable from the **KEYPAD** jack on the controller front panel into the electrical box and connect to the keypad jack.
- 5** Mount the keypad into the electrical box or retrofit bracket with the supplied screws.

Mode 2 Passcode Programming Procedure

When the keypad is in Mode 2, five memory slots on the keypad are available for programming. Slots 1 and 3 are used for Bypass codes. Slots 2 and 4 are used for Reset codes. A fifth slot is used for the Master Pass Code. The default codes assigned to the keypad memory slots are:

- Bypass: **1938**
- Reset: **1939**
- Master: **987654**

When you program the codes, you may use one code for both bypass slots and one code for both Reset slots, but you cannot use the same code for Bypass and Reset. Usually, you program separate codes and provide them to separate user groups.

To change the default **Bypass** or **Reset** codes, follow these steps:

- 1 Make sure the keypad has power.
- 2 Enter the Master Pass Code.
- 3 Press #.
- 4 Enter the slot number (1 or 3 for Bypass, 2 or 4 for Reset).
- 5 Press #.
- 6 Enter a new passcode (3 to 6 digits).
- 7 Press #.
- 8 Note the new passcode(s) and store in a safe place.

To change the default **Master Pass Code**, follow these steps:

- 1 Make sure the keypad has power.
- 2 Enter the Master Pass Code.
- 3 Press #.
- 4 Enter the Master Pass Code again.
- 5 Press #.
- 6 Enter a new passcode (3 to 6 digits).
- 7 Press #.
- 8 Note the new Master Pass Code and store in a safe place.

To restore a factory default code, follow these steps:

- 1 Make sure the keypad has power.
- 2 Enter the Master Pass Code.
- 3 Press #.
- 4 Enter the slot number (1 or 3 for Bypass, 2 or 4 for Reset).
- 5 Press #.
- 6 Do NOT enter a passcode.
- 7 Press # again.
- 8 The default passcode is restored.

Keypad Notes and Diagrams

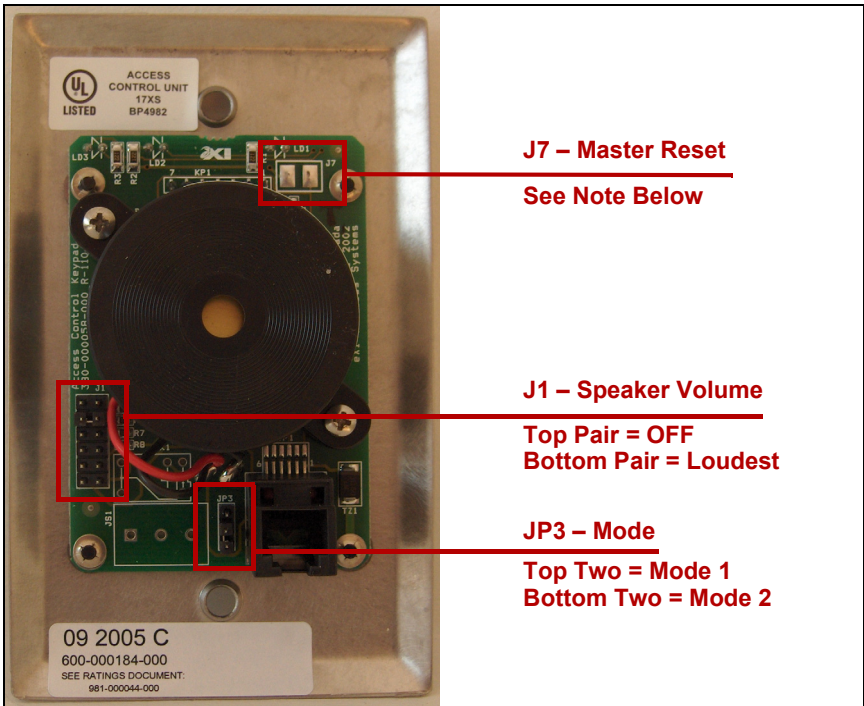


Figure 3-6: Keypad Jumper Locations

Master Reset

To reset the keypad to its factory default passcodes, follow these steps:

- 1 Apply power to the keypad.
- 2 Short the contacts on the J7 solder points at the upper right of the keypad back. The keypad will beep.
- 3 Press the * key three times. The keypad will beep to indicate that the defaults are loaded.

Installing a Wiegand Interface

The Xmark Wiegand interface allows you to substitute an appropriate card reader for the access keypad at a protected exit.

The Wiegand interface accepts standard 26-bit and other larger capacity Wiegand data formats. This eliminates the need for the staff member to carry a separate access card while at the same time remembering a PINcode for access to the same door.

The interface converts the Wiegand signal, which contains the access card ID, to a DTMF (Dual-Tone Multi-Frequency) signal and sends it to the R3 Controller. The Controller treats that signal the same way as a Mode 1 keypad signal.

The Wiegand interface has been designed and tested to work with HID Corporation proximity card readers (EntryProx, Thinline II, and other families) but can be used with any other equipment that generates Wiegand output in the same format.

Important: *When adding users to RoamAlert, the PIN code assigned to each user must be that user's access card ID (see the procedure "Add a New User" on page 4-29).*

Wiegand Interface Installation Tips

- **Identify the power requirements of the card reader.**

The door controller can provide power through the Wiegand interface to card readers that require +12V DC at 200 mA maximum current (150 mA if an access keypad is also powered by the controller).

Card readers that have different power requirements should be separately powered.

Note: *The Wiegand interface itself is powered by the keypad jack. If a keypad is being used along with the Wiegand interface, or if an auxiliary device is being connected to the interface, we recommend that you use a supplementary +12VDC power supply connected to the power terminals located on the back of the interface. See Figure 3-9 on page 3-20.*

- **Do not use the Wiegand pins (11 and 14) on the door controller terminal block.**

The interface communicates with the door controller through the keypad jack.

Wiegand Interface Installation Procedure

Follow these steps to install and test a Wiegand interface:

- 1 Mount the interface in a secure and accessible location.
- 2 Connect the **R3 CONTROLLER** jack on the back of the interface to the **KEYPAD** jack on the controller using a 6-conductor cable with **RJ11** plugs at each end.
- 3 Refer to Figure 3-8 on page 3-20. If the card reader will be powered by the controller:
 - 3.1 Connect the **PWR** pin and the **GND** pin on the back of the interface to Pins 3 and 4 (**+12V OUT** and **SYSTEM GROUND** respectively) on the door controller front panel.
 - 3.2 Connect **C-PWR** on the interface front panel to the red wire from the card reader.
 - 3.3 Connect **WGND0** on the interface front panel to the green wire from the card reader.
 - 3.4 Connect **WGND1** on the interface front panel to the white wire from the card reader.
 - 3.5 Connect **GND** on the interface front panel to the black wire from the card reader.
- 4 Refer to Figure 3-9 on page 3-20. If the card reader will be powered externally:

Note: *Do NOT connect C-PWR to the card reader in this scenario.*

 - 4.1 Connect **WGND0** on the interface front panel to the green wire from the card reader.
 - 4.2 Connect **WGND1** on the interface front panel to the white wire from the card reader.

- 4.3 Connect **GND** on the interface front panel to the black wire from the card reader.
- 5 Verify the interface connections. Look at the LED and compare its activity to this table:

LED	Interface Status
No activity	No power
Red-Yellow-Green cycle	Unit is powering up
Green	Power is on, both Wiegand lines are correctly connected and the interface is in idle mode
Red	Wiegand lines from reader not attached, reader is not powered up, or reader is malfunctioning
Blinking	Card has been read successfully and DTMF message sent to controller
Red 1 second, then Green	Card has not been read successfully (usually caused by swapped Wiegand lines). No DTMF sent to controller

Note: A “successful read” does NOT indicate that a correct passcode has been sent. The interface only sends the card information in a format (DTMF) that the controller can understand. The controller verifies the PIN code with the RoamAlert software. No confirmation is returned to the interface.

Wiegand Interface Notes and Diagrams

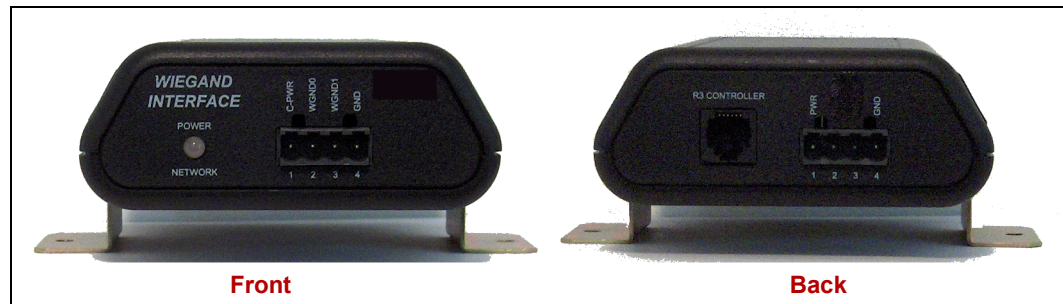


Figure 3-7: Wiegand Interface – Front and Back

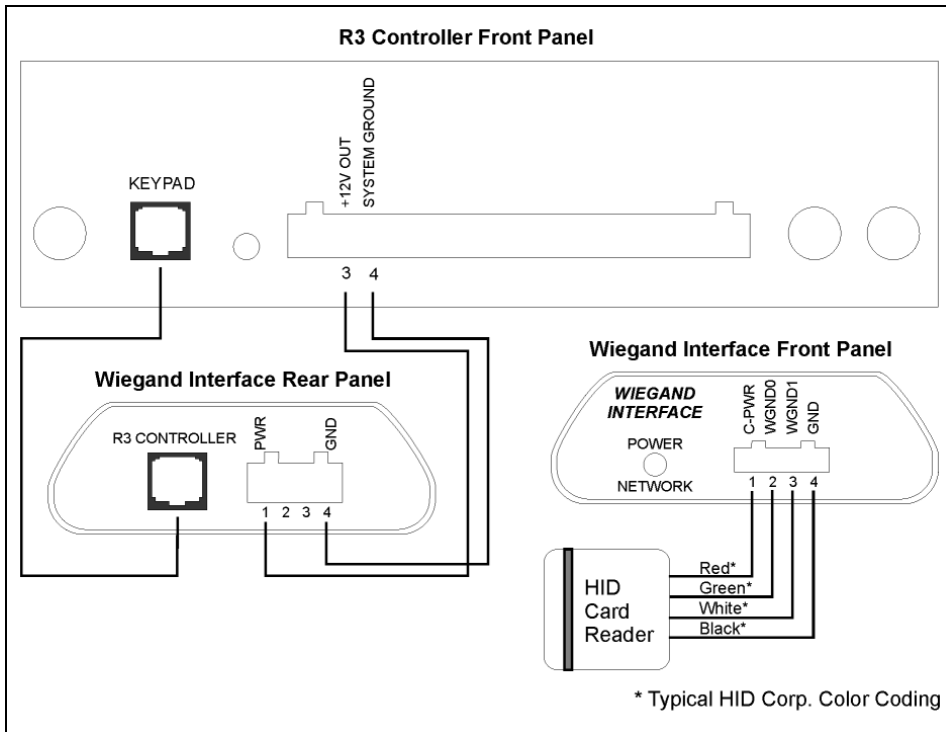


Figure 3-8: Wiegand Wiring Diagram (Card Reader Powered by Controller)

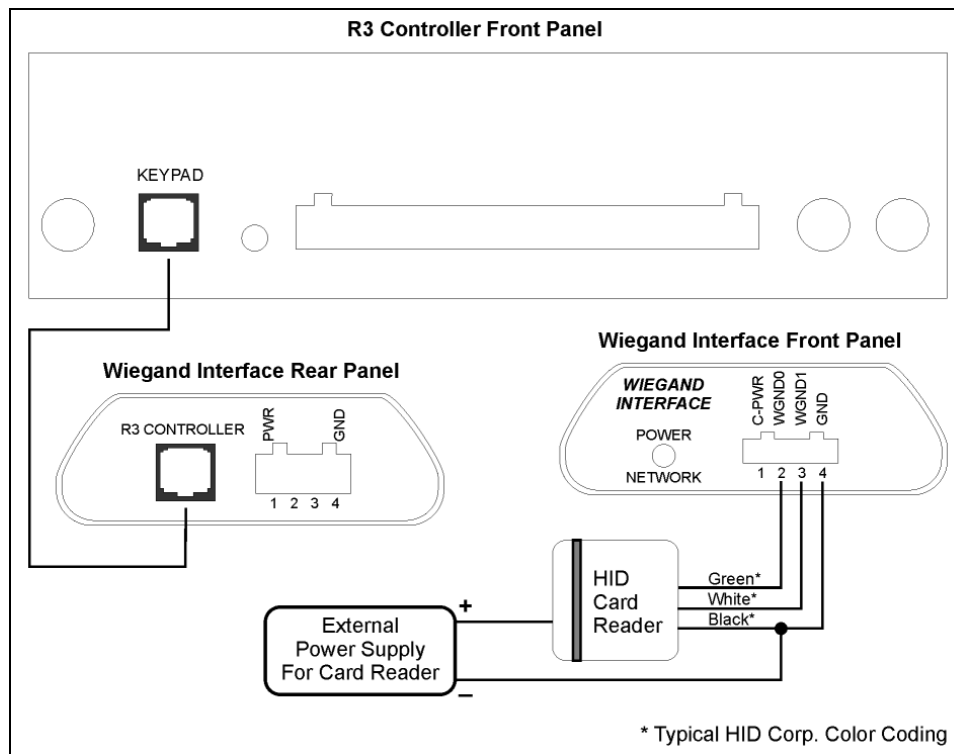


Figure 3-9: Wiegand Wiring Diagram (Card Reader Powered Externally)

Installing and Testing Receivers

This section describes the installation and testing procedures for R4 master receivers. For R3 receivers, refer to Appendix C – R3 Receiver Installation.

The R4 master receiver has two connectors on its base:

- a terminal strip connector for power, RS-485 host network, and an auxiliary output, and
- an RJ45 connector for RS-485 sub-network (reserved for future use).

A yellow status indicator LED is mounted on the circuit board under the translucent cover. The auxiliary output becomes active when a TIC (Tag Initiated Communication) message is received.

Receiver Installation Tips

- **Run network and power cables to each receiver location prior to installation.**
Leave at least 10 ft. (3 m) of slack, as adjusting the receiver's location may be required to optimize receive antenna reception.
- **Location is critical to detection accuracy.**
Mount the receiver away from metallic surfaces. Do not mount where metal will come between the receiver and tags. Common objects that may interfere with RF reception include:
 - water, earth, sprinkler, and heating pipes,
 - wire and wiring conduit, and
 - HVAC duct work and air diffusers.
 - other items not listed here.Other items not listed here may also cause interference. Inspect the environment thoroughly.
- **The receiver may be surface mounted.**
The receiver can be mounted directly to a wall or ceiling. Place the receiver where it is secure from casual theft or tampering. It can also be mounted above a dropped ceiling that does not have foil-backed tiles or other metallic interference. R4 receivers should only be mounted to ceiling tiles using standard single-gang electrical boxes or standard mounting straps.
- **Mount the receiver securely and with sufficient clearances.**
Use both mounting holes to secure the receiver. Locate the receiver so that you can position the antenna in any orientation depending on the environment.
- **Have an RF test tag handy.**
The RF test tag is used to test receiver coverage. The receiver beeps when it detects the test tag, but does not beep for any other tag.
- **Document the installed receiver.**
For each receiver installed, print and complete **Form 18**. Include this form in the System Commissioning binder.

Receiver Installation Procedure

Follow these steps to install an R4 master receiver:

- 1 Record the receiver's serial number on the facility floor plan at the correct location. This serial number is required during software configuration to identify the receiver. The serial number is found on the base of the receiver beneath the bar code.
- 2 Place the receiver at the approximate final location and position the antenna.
- 3 Connect the RS-485 cable: (see Figure 3-11 on page 3-23):

Note: *If it is absolutely necessary to use CAT-5e cable, it should be shielded.*

- 3.1** Connect the positive wire to **RS+** on the receiver terminal strip.
- 3.2** Connect the negative wire to **RS-** on the receiver terminal strip.
- 3.3** Connect the ground wire to **GND** on the receiver terminal strip.
- 4** Connect the 24 VDC power cable (see Figure 3-11 on page 3-23):
 - 4.1** Connect the red wire to **+V** on the receiver terminal strip.
 - 4.2** Connect the black wire to **GND** on the receiver terminal strip.
- 5** Verify the power and network wiring. Compare LED activity to this table:

LED	Receiver Status
No activity	No power
Slow dim flashing	Power applied, but no network communication
Continuous dim glow	Power applied, network communication OK
Bright flash	TIC, TIF, or TLM message
Three short high-intensity flashes followed by a long pause	Indicates Bootloader Mode. If persistent, may indicate a failure

- 6** Position the antenna. Point the tip away from any surfaces, including the receiver body and cables. Do not locate cables on the antenna side of the receiver.
- 7** Test the RF coverage to confirm effective detection range and identify dead spots:
 - 7.1** Hold the RF test tag button down.
 - 7.2** Move throughout the intended coverage area for this receiver.
 - 7.3** If the receiver beeps regularly, reception is good. Continue moving through the area.
 - 7.4** If beeping becomes irregular, reception is failing. This may indicate that:
 - you have reached the effective perimeter of the receiver detection range, or
 - the building structure or infrastructure is affecting reception.
- 8** If the structure or infrastructure is affecting reception, move the receiver or the antenna and repeat Step 6.
- 9** If you have reached the detection perimeter, record the coverage dimensions on the coverage or floor plan.
- 10** Permanently mount the receiver at the location confirmed in Step 7. If this is not a surface mount, install a single-gang electrical box, pass the cables through the box knockouts, and mount the receiver using two #6 screws. Refer to Figure 3-12 on page 3-24.
- 11** Move the antenna into its final position. Refer to Figure 3-10 on page 3-23.
- 12** Print and complete **Form 18**. Include this form in the System Commissioning binder.

Receiver Notes and Diagrams

The R4 Master Receiver automatically adjusts the reception threshold to reduce the effects of RF noise. Unlike the R3 receiver, manual adjustment is not required.

Abnormally high RF noise levels may cause a reduction in the receiver's detection range, but will not prevent the receiver from operating.

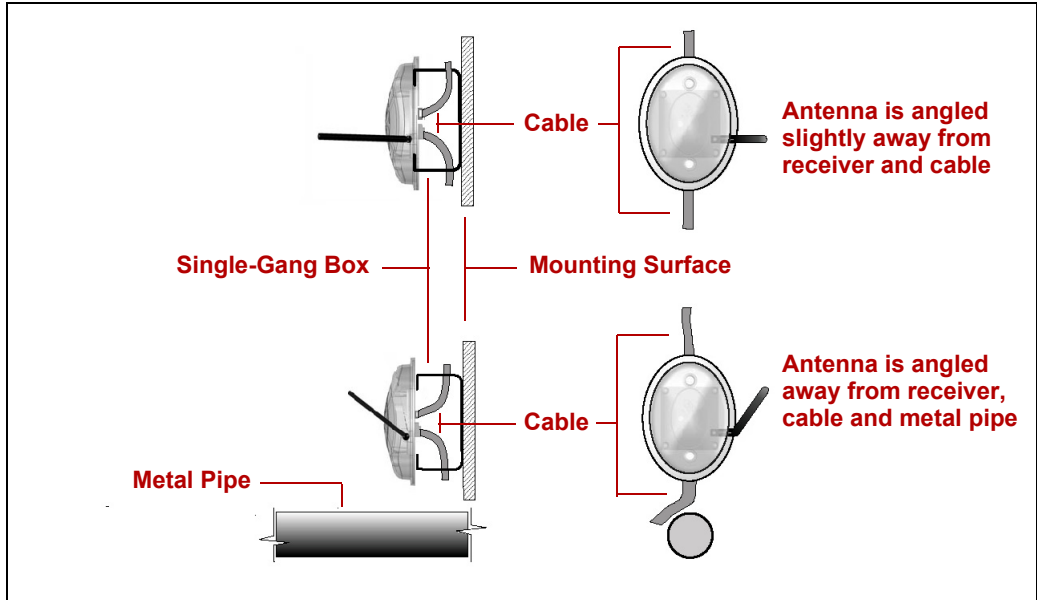


Figure 3-10: Antenna Orientation With and Without Adjacent Objects

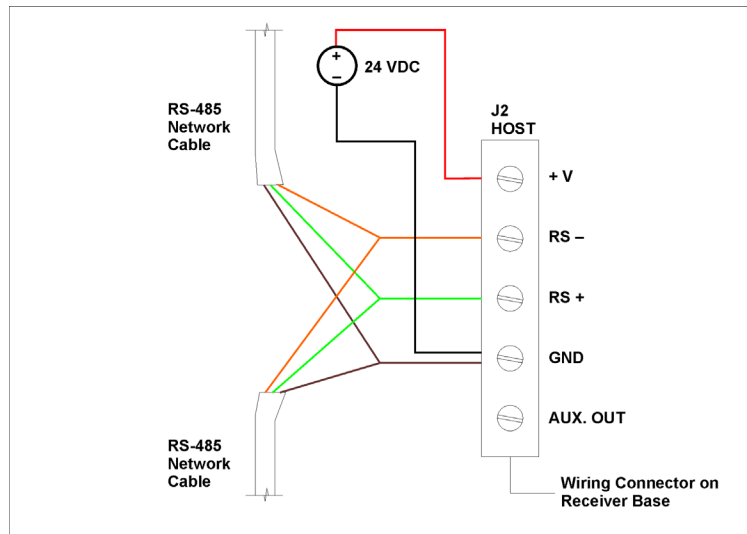


Figure 3-11: Receiver Wiring Diagram

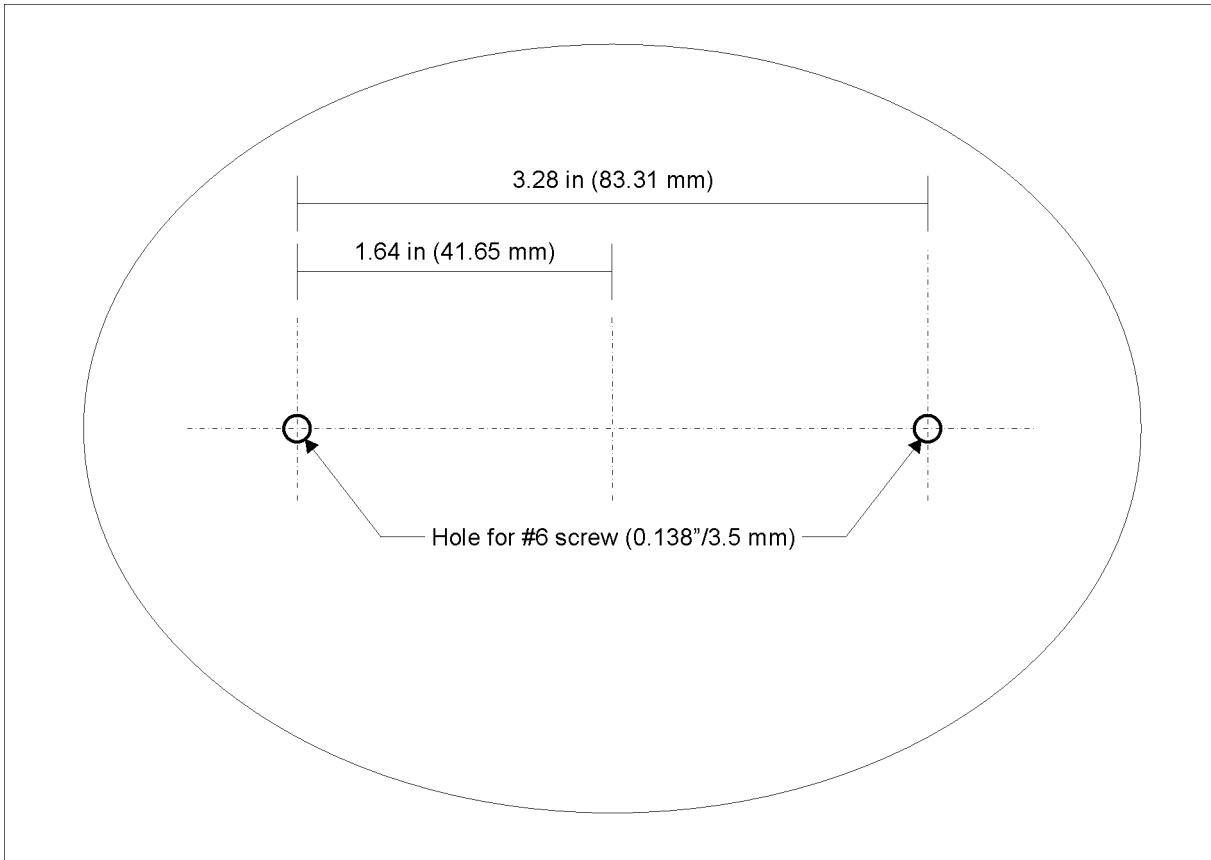


Figure 3-12: Receiver Mounting Template (Actual Size)

Installing and Tuning Elevator Control Systems

An elevator control system includes the following minimum components:

- one elevator cabinet with R3 controller, form C relay, power adapter and single-gang electrical box with adapter tie-down straps,
- two surface mount exciter antennas, each with 25' co-axial cable, template and screws,
- one receive antenna with 12' cable and alcohol prep pad,
- one access keypad, with 30' cable and one low voltage retrofit electrical box, and
- one 15' door switch cable.

Depending on the number of elevator cars, you will also need:

- one or more RS-485 repeaters (maximum 5 cars per repeater), and
- sufficient travelling cable to run from the repeater to each controller.

Important: *You must consult with the elevator maintenance company prior to installation. They will have specific requirements and schedules for the work.*

Elevator Control System Overview

The elevator control system looks like an R3 door controller placed inside a metal box with a pre-wired elevator control relay, power adapter, and power and cable entry holes with clamps. The elevator controller has its own tailored firmware and behaves much differently from the door controller. **The two controller types are not interchangeable.**



Figure 3-13: Elevator Control System Overview

System Layout

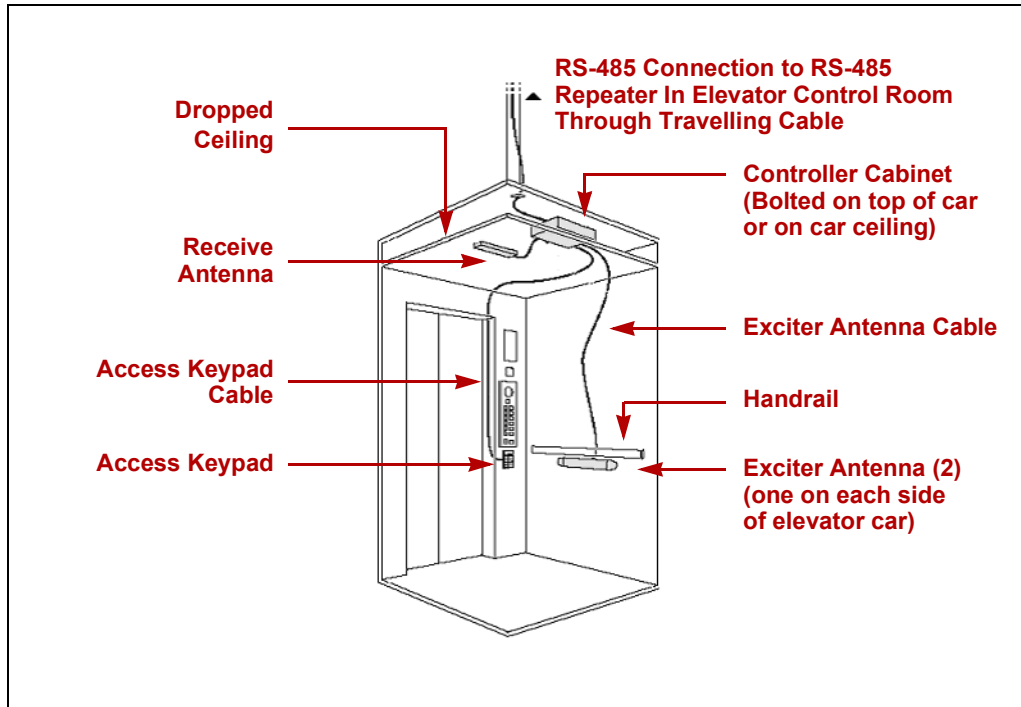


Figure 3-14: Elevator Control System Typical Layout

System Operation

• Detection Field

- The exciter antennas create a 307 KHz LF detection field in the elevator car only when the door is open.
- To turn the exciter field on when the door opens and off when the door closes, **DOOR SWITCH IN** (Pin 9) and **SYSTEM GROUND** (Pin 7) on the elevator controller must be connected to the elevator door switch contacts. In some older elevators these contacts may not exist, so a suitable set will need to be installed.
- As soon as a tag enters the car detection field, it transmits its identity to the elevator controller's receive antenna.

• Pre-Alarm

- When the controller identifies one or more tags in its detection field, it locks the car door open, and flashes the alarm light and sounds a warning tone on the access keypad.
- To lock the car door open, **MAGLOCK OUT 24V** (Pin 8) and **SYSTEM GROUND** (Pin 4) on the elevator controller must be connected to the elevator door control mechanism. The elevator controller is pre-wired to a form C relay in the cabinet for this purpose.
- If all tags are removed from the car or a bypass code is entered at the keypad within eleven (11) seconds, the alarm light and warning tone stop and the car door is allowed to close.

• Full Alarm

- If tags remain in the car longer than 11 seconds without bypass, or another tag enters the car after the bypass code has been entered, the system enters full alarm mode. The keypad

alarm light becomes continuous, the system sounds the full alarm siren and the door remains locked open until bypass is entered or the tags leave the car.

- **Bypass**
 - When bypass is initiated, the elevator door can close, and the car operates normally. Once the door has closed, the detection field is turned off.
Note: *asset tags will also transmit their identity if they are removed from the asset inside the car. This type of alarm (TIC) has no effect on elevator controller operation.*
- **Fire Condition Override**
 - In the case of a fire alarm, most elevators have a Fire Condition operating mode that seizes control of the elevator. For elevators that do not seize control, you can connect **OVERRIDE IN** (Pin 13) and **SYSTEM GROUND** (Pin 7) on the elevator controller to the fire condition contacts on the elevator control mechanism.

Elevator Control System Installation Tips

- **Install the cabinet with easy access in mind.**

Ensure that the cabinet can be opened fully to allow access to all components for testing, connection and adjustment.
- **Tune the exciter fields carefully.**

Tags must be detected anywhere in the car, without being detected in the elevator lobby. As well, exciter fields in adjacent cars must not intersect. Tune the fields until you achieve the absolute minimum field that will always detect a tag in the car.
- **Carefully test elevator bank installations.**

If exciter fields in adjacent cars in an elevator bank intersect, tags may not be reliably detected. Make sure each car is carefully tuned before testing the bank. If you still cannot reliably detect tags, please contact Xmark technical support for assistance.
- **Orient exciters correctly.**

The cable ends of both exciters in a car must be pointed in the same direction to prevent the fields from cancelling each other out.
- **Use repeaters to avoid noise on the network.**

If a noisy elevator shaft impedes network communications, installing additional repeaters at each controller cabinet will help to eliminate this interference.
- **Document the installed controller.**

For each elevator controller installed, print and complete **Form 17**. Include this form in the System Commissioning binder.

Elevator Control System Installation Procedures

Important: Most local building codes require that a qualified elevator technician install or approve all electrical and mechanical modifications to an elevator. In most cases, the elevator technician will do virtually all of the work described here.

Controller, Keypad, Wiring and Receive Antenna Installation

Follow these steps to install the controller, keypad, wiring, and receive antenna.

- 1 Record the elevator controller's serial number on the facility floor plan at the correct location. This serial number is required during software configuration to identify the controller. The serial number is found on a sticker at the inside lower left of the cabinet cover.
- 2 Mount the controller cabinet above the dropped ceiling inside the elevator car or outside on the car roof. The cabinet must be easily accessible for controller wiring and adjustment.
- 3 Unplug the AC adapter from the single-gang utility box inside the elevator controller cabinet.
- 4 Connect unswitched 110 VAC power to the utility box inside the cabinet.
- Access Keypad** 5 Mount the access keypad inside the car as follows:
 - 5.1 The recommended location is on the floor selection control panel at a convenient height for code entry. If there is no space on the panel, the car wall close to the panel will be suitable. A plastic low voltage electrical box is supplied with the keypad for retrofit installations.
 - 5.2 Cut a hole in the panel or wall 2" (500mm) wide by 2 7/8" (730mm) high to accommodate the back of the keypad.
 - 5.3 Drill holes for the screws, using the keypad as a template.
 - 5.4 Thread the keypad cable through the panel or wall up to the controller cabinet.
 - 5.5 Plug one end of the cable into the keypad's RJ11 jack and the other into the controller's **KEYPAD** jack. If you are mounting two keypads for a two-door elevator, first plug the Y-splitter (supplied with the keypad kit) into the controller's **KEYPAD** jack.
 - 5.6 Secure the keypad to the panel or wall.
- Door Status** 6 Connect to the elevator door status contacts as follows:

Note: It may be preferable to tie into the elevator door close limit switch.

 - 6.1 If the elevator does not have door status contacts, install a suitable set of contacts on the door. These contacts should be normally open (NO) when the door is open.
 - 6.2 Connect a pair of wires from **DOOR SWITCH IN** (Pin 9) and **SYSTEM GROUND** (Pin 7) on the elevator controller to the door switch **NO** and **COMMON** contacts.
 - 6.3 If the elevator door contacts are normally closed (NC) when the door is open, you need to set JP302 on the elevator controller board. See "Elevator Controller Jumpers and Switches" on page 3-36
- Door Control** 7 Connect to the elevator door control mechanism as follows:
 - 7.1 Connect a pair of wires from terminals 7 and 8 on the form C relay in the cabinet to the appropriate door open control contacts on the elevator control panel. **MAGLOCK OUT 24V** (Pin 8) and **SYSTEM GROUND** (Pin 4) on the elevator controller are pre-wired to the form C relay inside the controller cabinet.
- Door Lock Disable** 8 If the elevator does not automatically disable the door lock during a fire alarm (most do), connect to the elevator's fire alarm contact as follows:

- 8.1** Connect a pair of wires from **OVERRIDE IN** (Pin 13) and **SYSTEM GROUND** (Pin 7) on the elevator controller to the elevator's normally open fire alarm contact.
- RS-485 Network** **9** The RS-485 network should already be routed through the elevator control room. Connect the elevator controller to the network as follows:
- 9.1** Connect one side of an RS-485 repeater to the RoamAlert RS-485 network in the elevator control room. If there are more than five (5) elevators being controlled, more repeaters will need to be connected.
- 9.2** Run a three (3) conductor shielded, stranded, low capacitance travel cable (Draka WSCC 6x20 SH ID #18-003-15 recommended) to the controller cabinet and connect to **RS-485+** (Pin 5), **RS-485-** (Pin 6) and **SYSTEM GROUND** (Pin 4) on the controller.
- 10** Plug in the power adapter that you unplugged in Step 3, and use the supplied tie-down straps to secure the adapter against vibration and movement.
- Receive Antenna** **11** Mount the receive antenna horizontally on or above the dropped ceiling, parallel to the car floor and centered in the car, as follows:
- 11.1** Locate a suitable position. Above a dropped ceiling is best provided that the antenna is not shielded from the car by foil-backed ceiling panels, metal fans or duct work, light fixtures, metal-coated diffusers, or other metal or metal-coated objects.
- 11.2** Temporarily mount the antenna at the selected location and connect the cable to the **RECEIVE ANTENNA** jack on the front of the controller in the cabinet.
- 11.3** Ensure that there are no tags in the area. Turn off all elevator and door controllers within 20 feet of the elevator being adjusted.
- 11.4** Set the **Receiver Sensitivity** switch (**SW201**) on the controller circuit board (bottom left) to maximum sensitivity (9). The **Receive Indicator** (**LD501**) at the upper left of the controller board flickers each time a random noise signal is received.
- 11.5** Turn the switch counter-clockwise one number at a time to reduce receive sensitivity until the indicator stops flickering. (It is normal for the LED to flicker once every three or more seconds without compromising operation.)
- 11.6** If you have to set the switch below 4, coverage may be compromised. Move the antenna slightly and perform Steps 11.3 and 11.4 again.
- 11.7** When you are satisfied with the receive sensitivity setting, mark the antenna location.
- 11.8** If the antenna is below the dropped ceiling, drill a suitable hole to accommodate the BNC connector at the marked location, and place a grommet into the hole to protect the cable from fraying or other damage.
- 11.9** If the controller is on top of the car roof, also drill a suitable hole through the car roof and fit a grommet into the hole.
- 11.10** Clean the mounting surface with supplied alcohol prep pad or a similar cleanser.
- 11.11** Remove the protective strip from the antenna's adhesive backing and mount the antenna firmly to the surface.
- 11.12** Thread the cable through the grommetted hole(s) and connect it to the **RECEIVE ANTENNA** jack on the front of the controller in the cabinet.
- 12** Print and complete **Form 17**. Include this form in the System Commissioning binder.

Tuning the Exciter Fields

In most cases, both exciters in an elevator car will be positioned horizontally on the side walls, 1-2” under the handrail and exactly centered between the ends of the car. The cable ends of the exciters must point in the same direction to prevent the fields cancelling each other out.

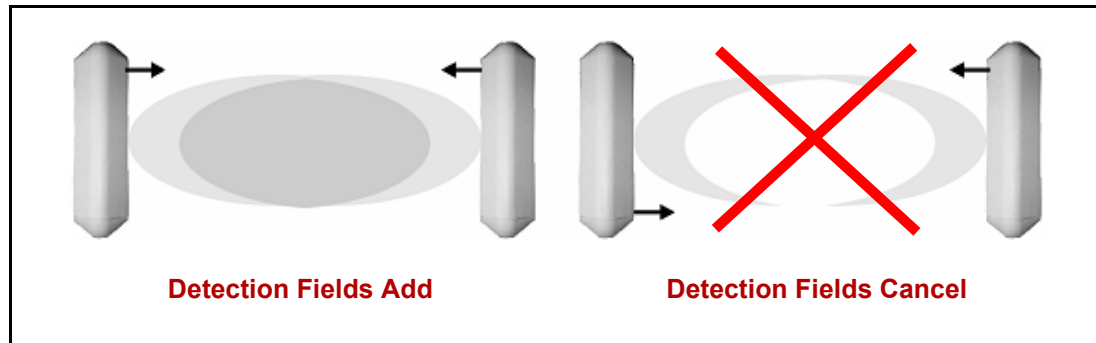


Figure 3-15: Exciter Antenna Orientation

The exciter detection field must be adjusted so that no tag can enter the car without being detected, while keeping the field from extending outside the car when the door is open to prevent false alarms from tags in the elevator lobby.

Due to environmental factors, there may be situations where the recommended location will not provide suitable detection field coverage. Therefore, in this procedure we suggest that you position the exciters temporarily until they are successfully tuned before mounting them permanently. Where you are installing in a bank of elevators, tune each individual car, then tune the entire bank before permanently mounting the exciters.

Single-Car Tuning

Follow these steps to tune the exciter antennas in a single elevator car:

- 1 Turn off all elevator and door controllers within 20 feet of the elevator being tuned.
- 2 Attach the cables to the exciters and temporarily mount them in the recommended location.
- 3 Route the cables to the controller and connect them to **SRA #1** and **SRA #1** on the controller front panel.
- 4 Set the **Mode** switch (**SW102**) on the controller board to position 0 (test mode). The keypad will beep continuously when a tag is detected and stop when the tag is no longer detected.
- 5 Use one of these three methods to tune the exciter field:
 - Method 1 (recommended):
 - 5.1 Turn switch **R520** (the large blue potentiometer at the upper right of the controller circuit board) to the middle position.
 - 5.2 Turn switch **SW201** (the beige switch near the lower left of the controller circuit board) to position 4 (medium sensitivity).
 - 5.3 Use an RF test tag or a pocket tag reader to establish the presence of an exciter field.
 - 5.4 Move a tag throughout the elevator car and listen for the beeping. Test the tag in various horizontal and vertical orientations and do not forget the floor. If there are areas where the tag is not detected at this setting, turn **R520** clockwise to increase the exciter field size, then test again. If the tag is detected in all locations, turn **R520** counter-clockwise to reduce field size, then test again.

- Method 2:

- 5.1** Turn switch **R520** (the large blue potentiometer at the upper right of the controller circuit board) fully clockwise to maximize the size of the detection field.
- 5.2** Move a tag throughout the elevator car and listen for the beeping. Test the tag in various horizontal and vertical orientations and do not forget the floor. If there are areas where the tag is not detected at this maximum setting, move the exciters to a different location and repeat the test. If the tag is detected in all locations, turn R520 counter-clockwise 1/8 of a turn to reduce field size.
- 5.3** Repeat Step 5.2 until there are areas where the tag is not detected. Turn switch **R520** clockwise 1/8 turn to go back to the last setting where the tag was always detected. The detection field will now be at the optimum size necessary to always detect tags in the car while minimizing false alarms from tags outside the car.

- Method 3:

- 5.1** Turn switch **R520** (the large blue potentiometer at the upper right of the controller circuit board) counter-clockwise until the DC voltage at **TP502** (Test Point 502) is set to 5.5V.
- 5.2** Move a tag throughout the elevator car and listen for the beeping from the keypad. Test the tag in various horizontal and vertical orientations and do not forget the floor. If there are any areas where the tag is not detected, turn switch R520 clockwise to increase the voltage by 1 or 2 volts and retest the tag.
- 5.3** Repeat Step 5.5 until the tag is always detected. The detection field will now be at the optimum size necessary to always detect tags in the car while minimizing false alarms from tags outside the car.

- 6** If this is a single-car installation set the **Mode** switch (**SW102**) on the controller board back to its operating position and continue with the section “Permanently Mounting the Exciters” on page 3-32. Otherwise, repeat this procedure for each car in an elevator bank, then continue with the section “Bank Testing” below.

Bank Testing

Occasionally, due to environmental factors, elevators that are adjacent may interfere with each other if the exciter fields are intersecting outside the cars and, in extreme cases, within the cars. A tag entering one of the cars may see these two fields as a noise source and not respond to either. For this reason, adjacent cars in the bank must be tested together. If, following rigorous testing, you are unable to successfully tune the elevator bank, please contact Xmark technical support for assistance.

- 1** After all individual cars in the elevator bank have been successfully tuned, turn on all controllers in the bank and turn on any nearby door controllers.
- 2** Call the first two cars to the same floor and open both doors.
- 3** Enter each car with a tag and monitor the elevator controller’s response. If the response is diminished in either car with the adjacent door open, increase receive antenna sensitivity slightly (**SW201**) and test again. If you are absolutely unable to test successfully, please contact Xmark technical support for assistance.
- 4** If there are more than two cars in the bank, release the first car and call the third car to the floor and open the doors. Repeat Step 3 for these two cars and continue in this fashion until all cars in the bank have been tested.
- 5** When all cars in the bank have been successfully tested, continue with the section “Permanently Mounting the Exciters” below.

Permanently Mounting the Exciters

In some cases, the facility may not want the exciter antenna to be exposed. In this situation, you must ensure that the exciter is not mounted behind metal.

Follow these steps to permanently mount each exciter:

- 1** Remove the center section of each exciter cover by spreading the sides to release them from the base.
- 2** Center the mounting template (supplied with each exciter inside the center cover) horizontally on one side wall at least 1” below the handrail (or at the location discovered during testing), and mark the screw and co-axial cable entry holes.
- 3** **Making sure to orient the template in the same direction**, center the template on the other side wall at the same height and mark the screw and co-axial cable entry holes.
- 4** Drill suitable holes for the mounting screws and cable, and place grommets into the cable holes to protect the cable from damage.
- 5** Connect the exciter cables to **SRA #1** and **SRA #2** on the controller front panel, and feed the cables from the controller cabinet down into the car walls, and out through the grommeted cable holes.
- 6** Attach the cables and mount the exciter to the wall using the supplied screws.
- 7** Replace the exciter covers by snapping them into place.

Elevator System Notes and Diagrams

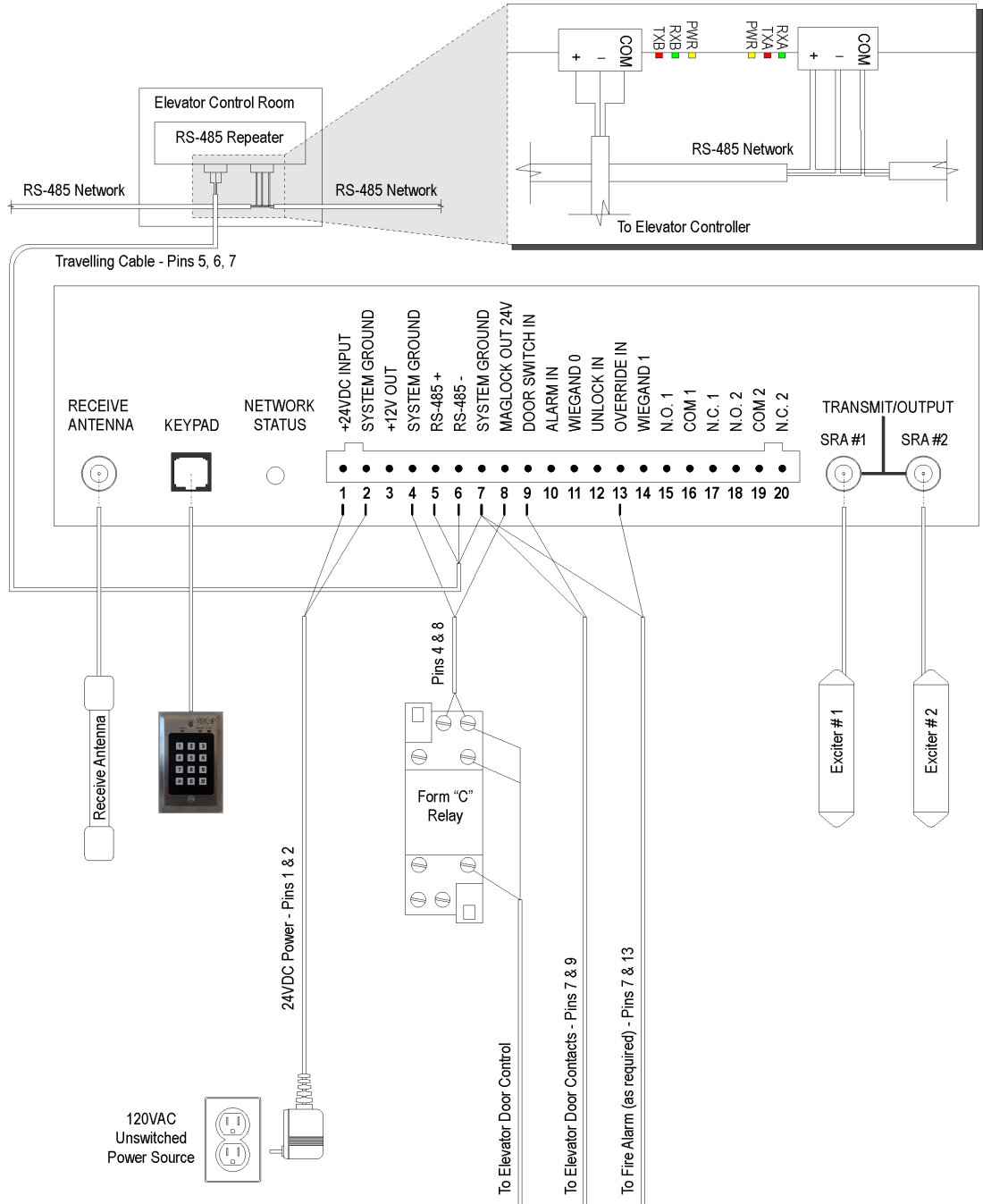


Figure 3-16: Elevator Wiring Diagram

Table 3.4 Elevator Controller Front Panel Connectors – Left to Right

#	Name	Remarks
–	Receive Antenna	BNC connector for cable antenna. Do not exceed 15 feet of RG58 antenna cable.
–	Keypad	RJ-11 connector for keypad. Two keypads can be connected using a modular Y adapter (Part # AR3KA01-001)
1	+24VDC INPUT	Powers the controller (250 mA) and +12 VDC auxiliary output (200 mA max).
2	SYSTEM GROUND	Common Ground
3	+12V OUT	Power for auxiliary devices (12VDC, 200mA max)
4	SYSTEM GROUND	Common Ground for 12VDC auxiliary power output
5	RS-485 +	Network connectors to the RS-485 repeater in elevator control room
6	RS-485 -	
7	SYSTEM GROUND	Ground for RS-485 and MAGLOCK OUT 24V. Select one device only for RS-485 ground.
8	MAGLOCK OUT 24V	Power (24 VDC, 1.0A max) to energize the car door disable relay whenever a tag is in the detection zone and the car door is open
9	DOOR SWITCH IN	Active low signal (ground), activates the alarm relays and keypad alarm indicators while the door is open and a Tag is in the detection zone. For elevator cars with front and back doors, connect door switches in series (NC contacts) to System Ground so that opening either door activates the alarm when a tag is in the detection zone. See jumper JP302 in Table 3.5 below.
10	ALARM IN	Not used
11	WIEGAND 0	Not used
12	UNLOCK IN	Not used
13	OVERRIDE IN	Deactivates the car door lock, audible alarm, and keypad alarm indicators when connected to system ground, even if the car door is open and a Tag is in the detection zone; typically connected to the fire alarm contacts in the car to disable the controller during a fire.
14	WIEGAND 1	Not used
15	N.O. 1	Alarm Relays 1 and 2 are activated when the car door is open and a tag is in the detection zone for more than 11 seconds. Alarm Relays 1 and 2 are deactivated when all tags leave the detection zone, when a bypass code is entered at the keypad, or when OVERRIDE IN is connected to system ground. Maximum relay contact current is 2A @ 30 VDC.
16	COM 1	
17	N.C. 1	
18	N.O. 2	
19	COM 2	
20	N.C. 2	
–	SRA #1	BNC connectors for two exciter antennas. Do not exceed 25 feet of RG59 cable for each antenna.
–	SRA #2	

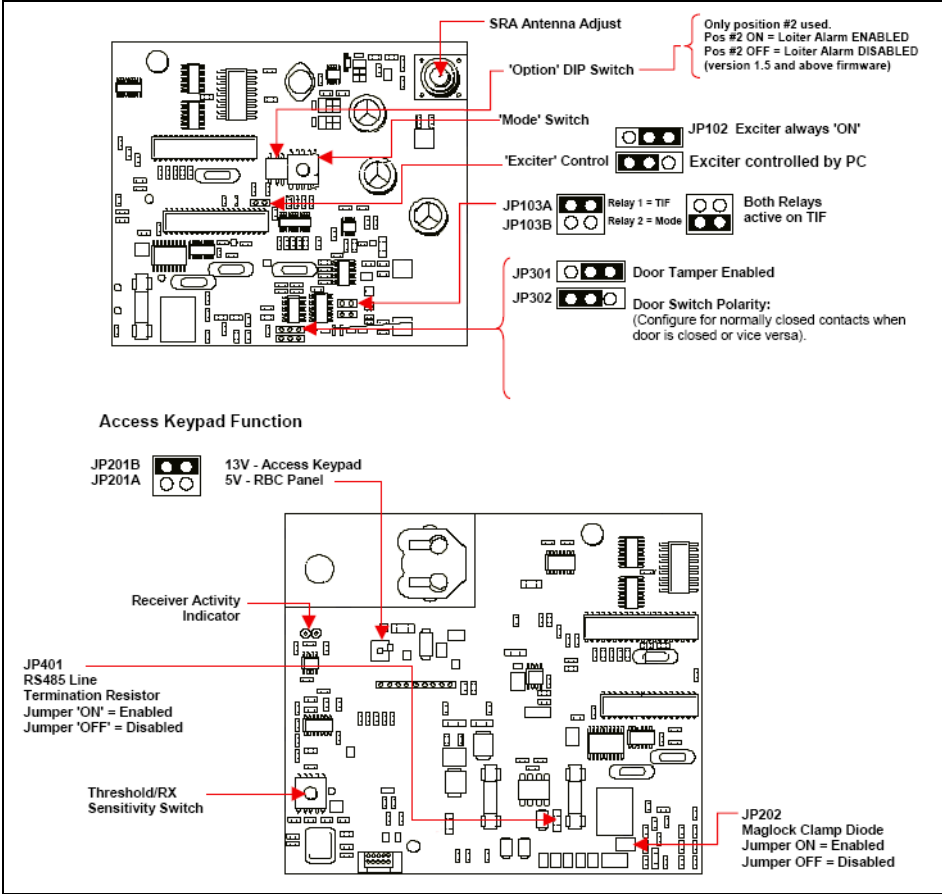


Figure 3-17: Elevator Controller Jumpers and Switches

Table 3.5 Elevator Controller Jumpers and Switches

Label	Default	Description	Remarks
JP102	Pos 1-2	Pos 1-2 – Exciter always on Pos 2-3 – Exciter controlled by PC	Do not change default setting.
JP103A JP103B	Pos B	Pos A – Relay 1 = TIF, Relay 2 = Mode Pos B – Both relays active on TIF	Do not change default setting.
JP201A JP201B	Pos B	Pos B – 13V - Access Keypad Pos A – 5V - RBC Panel	Do not change default setting.
JP202	OFF	For Maglock. Not used with elevator	Do not change default setting.
JP301	Pos 1-2	For door tamper. Not used with elevator	Do not change default setting.
JP302	Pos 2-3	Pos 2-3 – Meant for contacts that are closed when the door is closed . Pos 1-2 – Meant for contacts that are closed when the door is open .	
JP401	OFF	OFF – RS-485 line termination resistor disabled ON – RS-485 line termination resistor enabled	Do not change default setting.
LD501	N/A	Receive indicator: lights momentarily each time a tag is detected. Flickers intermittently if random RF noise signal is received.	Located at the upper left of the board, used for testing receive antenna reception during installation.
SW102	Pos 3	Controller mode switch: Pos 3 = Unlatched – alarm automatically terminates	See Table 3.6 for mode switch settings.
SW103	SW 2 ON	SW 2 ON – Loiter alarm enabled SW 2 OFF – Loiter alarm disabled	SW 1 is not used.
SW201	Pos 4	Receiver threshold switch: adjust for optimum noise suppression and tag reception. 0 = OFF, receiver disabled 1 = low sensitivity, high noise suppression 7 = high sensitivity, low noise suppression 8, 9 = highest sensitivity, no noise suppression	
R520	N/A	Exciter antenna adjust: controls the power of the exciter field. Turn clockwise to increase the field power and detection zone size.	Do not set a detection zone larger than 10 feet.
Network Status (on front panel)		OFF – no power to controller. Solid green – Normal operation and RS-485 network communication. Solid red – RS-485 network communication never established. Flashing red/green – RS-485 network communication established, then lost.	

Table 3.6 Elevator Controller Mode Switch (SW102) Settings and Relay Action

Position	Description	Relay Action	
		Relay 1	Relay 2
0	Test mode. Use only while testing during installation or troubleshooting.	No action	No action
1	Non-latched alarm – automatically terminates	Active TIF D/O	Active TIF D/O
2	Latched alarm – does not terminate	Active TIF D/O	Active TIF D/O
3	Non-latched alarm – automatically terminates	Active TIF D/O	TIC
4	Latched alarm and pre-alarm	Active TIF D/O	TIC
5	Non-latched alarm – automatically terminates	Active TIF D/O	Active on Bypass
6-9, A-F	Not used.		
		D/O = Door Open, D/C = Door Closed TIF = Tag In Field (in exciter detection zone) TIC = Tag Initiated Communication (tamper)	

Installing an I/O-8 Module

The I/O-8 Module provides an interface for a variety of peripheral devices. The module has eight ports that can be programmed to function as either inputs or outputs, hence the name I/O-8.

The I/O-8 Module allows your resident wandering/asset protection system to also operate as a perimeter security system. For example, a RoamAlert system can monitor dry contact or voltage changes if the signal is connected to an input on the I/O-8 Module.

RoamAlert triggers output ports on the module based on four possible input types:

- **Time triggers** cause output ports to be activated at specified times during a day. For example, a time trigger can activate an output port that engages a connected maglock from 8:00 pm to 6:00 am every day.
- **Event triggers** cause output ports to be activated when a system event happens. For example, an event trigger can activate an output port when an off-body (TIC) or exit alarm (TIF) occurs at a specific node.
- **Link triggers** cause output ports to be activated when an input port is activated. For example, a link trigger can monitor the area at an exit when an event occurs, such as the door being opened if the door switch is also connected to an input port on the module.
- **Combination triggers** cause output ports to be activated when a link or event trigger condition is met during a specified time period.

The triggers for the I/O-8 module are defined in the RoamAlert software. Refer to “Add Links” on page 4-50 for configuration details. If you are using system events as triggers, also refer to “Add Links” on page 4-50.

Module Features

- 8 ports configurable as supervised inputs or outputs in any combination,
- Monitored zones when configured as inputs (EOL),
- Sinking outputs (500 mA total load),
- Latching and non-latching programmable inputs,
- Normally open and normally closed inputs,
- Zone links: Time triggered, system event triggered. Zones can respond to an input, in which case a change of state will cause annunciation at the server PC.
- An LED indicator displays power (green when on) and RS-485 activity (red during activity).

I/O-8 Module Installation Tips

- **Carefully plan the location of the I/O-8 module.**
Know where the input and output zones will be and centrally locate the module.
- **Run network and power cables to each module location prior to installation.**
Leave at least 10 ft. (3 m) of slack for module location adjustments.
- **Output ports are restricted to a 500mA total load.**
Each port can output up to 100mA at 24VDC.
- **Power the module from the central power supply.**
The I/O-8 module requires 24VDC / 800mA of power.

- **Document the installed module.**
For each module installed, print and complete **Form 6**. Include this form in the System Commissioning binder.

I/O-8 Module Installation Procedure

Follow these steps to install and test an I/O-8 module:

- 1 Record the module's serial number on the facility floor plan at the correct location. This serial number is required during software configuration to identify the module. The serial number is found on the underside of the module beneath the bar code.
- 2 Connect the inputs and outputs. See Figure 3-19 and Figure 3-20 on page 3-41.
- 3 Connect the RS-485 cable (see Figure 3-18 on page 3-40):
 - 3.1 Connect the positive wire to **RS-485 +** on the module's front terminal strip.
 - 3.2 Connect the negative wire to **RS-485 -** on the module's front terminal strip.
 - 3.3 Connect the ground wire to **GND** on the module's front terminal strip.
- 4 If this is the last device in an RS-485 chain, a terminator must be installed.
- 5 Connect the 24 VDC power cable (see Figure 3-18 on page 3-40):
 - 5.1 Connect the red wire to **PWR** on the module's front terminal strip.
 - 5.2 Connect the black wire to **GND** on the module's front terminal strip.
- 6 Verify the power and network wiring. Compare LED activity to this table:

LED	I/O-8 Module Status
No activity	No power
Alternating red and green	Power applied, but no network communication
Continuous green	Power applied, network communication OK

- 7 Test each connected input and output after software configuration. Refer to these sections for complete configuration details:
 - “Add and Configure Nodes” on page 4-13, and
 - “Add Links” on page 4-50 (if using system events as triggers), and
- 8 Print and complete **Form 6**. Include this form in the System Commissioning binder.

I/O-8 Module Notes and Diagrams

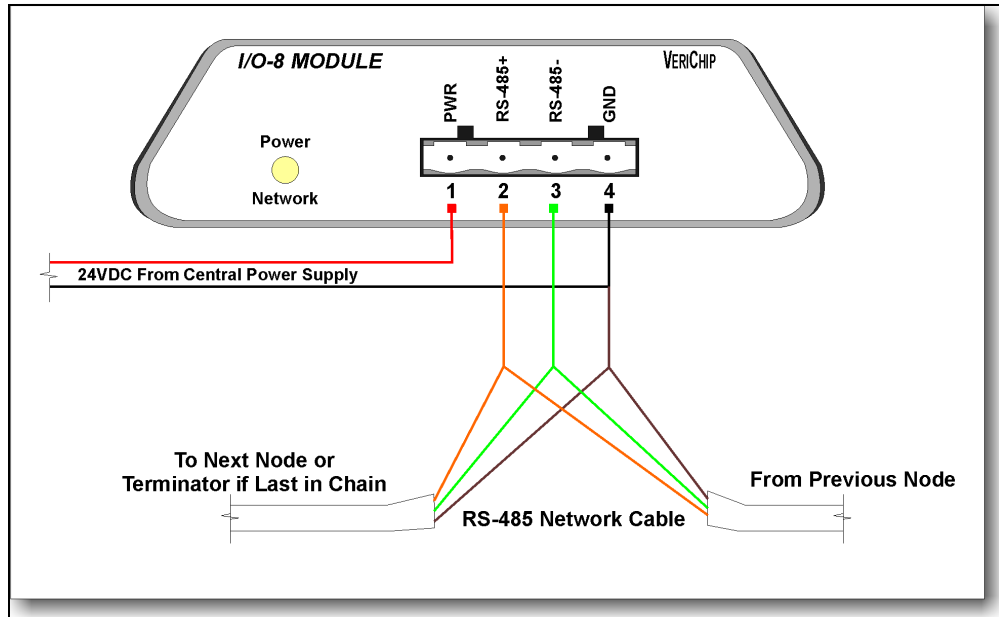


Figure 3-18: I/O-8 Module System Connections

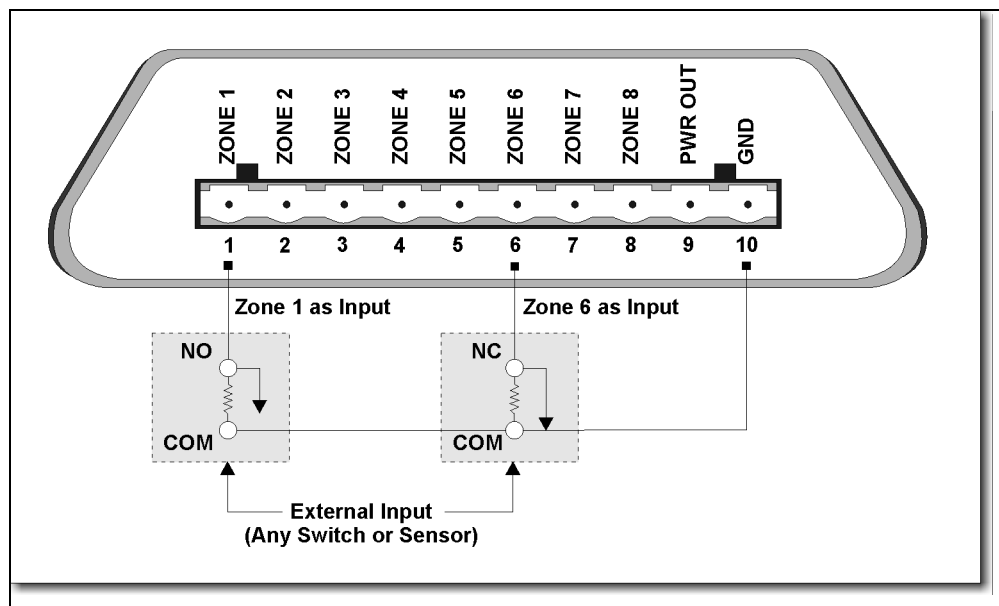


Figure 3-19: I/O-8 Module Typical Input Wiring

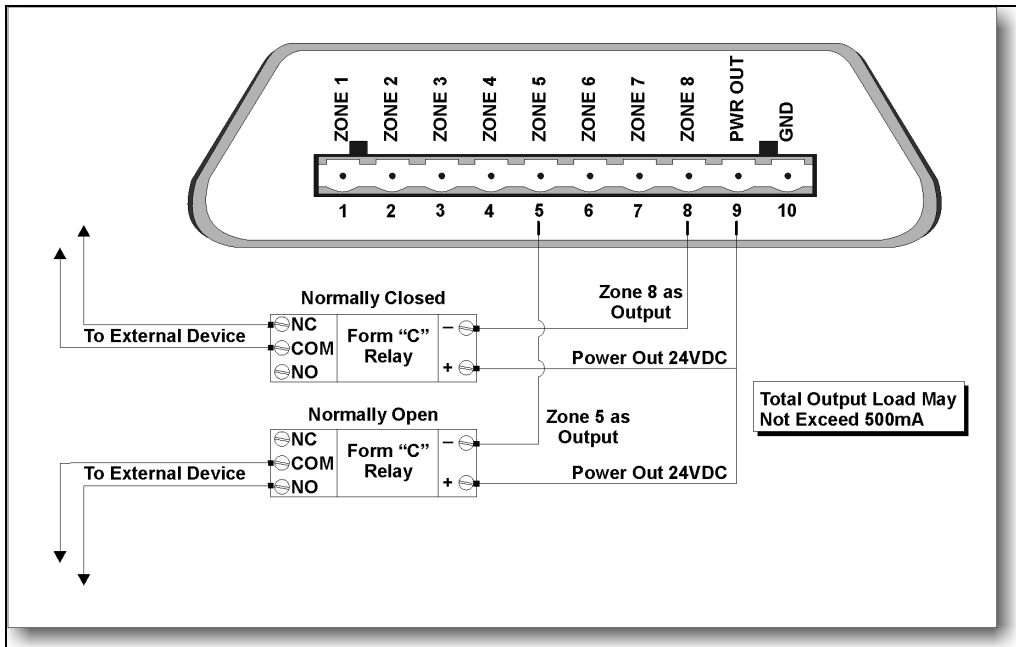


Figure 3-20: I/O-8 Module Typical Output Wiring

Installing an Alarm Output Module

The Alarm Output Module allows RoamAlert to activate external devices through one of two relays when either an exit alarm (Tag In Field - TIF) or off-body alarm (Tag Initiated Communications - TIC) alarm is triggered. The Alarm Output Module uses the RS/EIA-232 protocol and connects to the 9-pin serial port of a PC.

An alarm output module can be connected to either a server PC or a console PC. The console properties in the RoamAlert software must be configured to reflect the installation of the module.

Relays

When an alarm is received at the console, the module relays are switched from NC (Normally Closed) to NO (Normally Open). Each relay contact is an **OMRON G5S-1 DC12**, which is rated for 3A @30VDC for a closed contact.

LED Status

An LED for each relay indicates the state of that relay: green for power-on and no alarm, and red when an alarm is activated.

Dip Switches

A two-position DIP (Dual Inline Package) switch (1=TIF, 2=TIC) is used to configure the module's response to disconnection of the serial port or powering down of the console. An OPEN (OFF) DIP switch fires the corresponding TIF or TIC relay when the serial port is disconnected while RoamAlert is running or the PC is powered down. A CLOSED (ON) DIP switch does not fire the corresponding relay.

Serial Connections

As stated, the alarm output module connects to the PC's 9-pin serial port. Also, provided on the module is a 9-pin serial port for pass through purposes. If another device, such as a local printer, is using the PC's serial port, the device can be "daisy-chained" through the module.

Note: Normally, an RS232 device is a single host to client receiver, and only one client is allowed to be hosted by an RS232 serial connection. However, the alarm output module is not actually a serial device, so it does not establish serial communication with the computer. Instead, the module relies on two connections, DTR (Data Terminal Ready) and RTS (Request To Send) for its operation. Therefore, as long as a serial device does not use DTR and RTS (such as a TagLink or Tag Reader), then it can be plugged into the module's pass-through serial port.

Alarm Output Module Installation Tips

- **Power the module according to the need.**
If it is critical that the module operate at all times, power it from the RoamAlert central power supply, otherwise a 12VDC @ 1A power adapter may be used.
- **Locate the module for easy visual access.**
The module LEDs should be visible to anyone working at the console. The module is designed to rest on the surface next to the console, however, a bracket could be used for wall mounting.

Alarm Output Module Installation Procedure

Follow these steps to install and test an alarm output module:

- 1 Connect the **PC COM. PORT** on the module to an available serial port on the console using a 9-pin RS-232 serial cable.
- 2 Connect the external device to the appropriate (TIF or TIC) relay terminal blocks. If you want the device to respond when an alarm occurs, connect it to **NO** and **COMMON**. If you want the device to stop responding when an alarm occurs, connect it to **NC** and **COMMON**.
- 3 Set the DIP switches for the desired response to a console power down or serial port disconnection condition. Switch 1 controls TIF and switch 2 controls TIC. Set the appropriate switch ON (CLOSED) to cause the corresponding relay to ignore power down or disconnection, or OFF (OPEN) to activate that relay.
- 4 Connect a 12VDC @ 1A power adapter to a local 120VDC receptacle and the power jack on the module.
- 5 Verify the power and serial port connections. Compare LED activity to this table:

LEDs	Module Status
No activity	No power
Both green	Power applied, no alarm conditions
Either red	Alarm condition, also console power down or serial port disconnection (dependent on DIP switch settings)

- Important:** 6 During the configuration phase, make sure to adjust the console property sheet in the RoamAlert software to identify the serial port and notification settings for the module. See “To Adjust the Configuration of the Server PC (or any console)” on page 4-23 for details on this step.

Alarm Output Module Notes and Diagrams

Specification	Rating
Relay Coil Voltage	12VDC
Relay Coil Current	33.3mA
Max Switching Voltage	277VAC / 30 VDC
Max Switching Current (resistive load)	2A (NO) / 2A (NC) @ 277VAC 5A (NO) / 3A (NC) @ 125VAC 5A (NO) / 3A (NC) @ 30VDC
Max Switching Current (inductive load)	0.5A @ 250VAC, cosf = 0.4 1.0A @ 250VAC, cosf = 0.8 0.8A @ 250VAC, cosf = 0.9

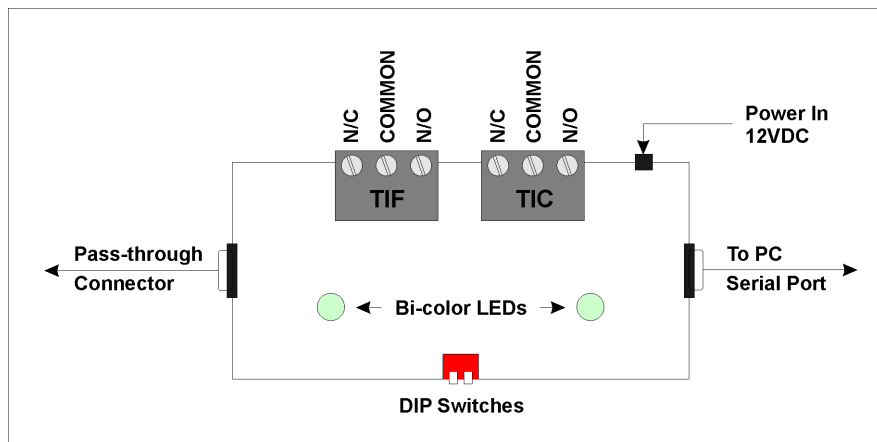


Figure 3-21: Alarm Output Module Block Diagram

Installing a Remote Display Unit (RDU)

The RDU is most useful in a large installation, particularly in situations where a console PC is not practical or necessary. It is typically mounted near a remote exit where users may need to accept alarms but not need full console functionality. The RDU can be connected in either local or non-local configurations. In a non-local configuration the RDU is connected only to the RS-485 network and is used to remotely monitor system status and accept alarms. In a local configuration, the RDU is also connected to a door controller and can replace a keypad for bypass functions.

The RDU can be configured for HIPAA (Health Insurance Portability and Accountability Act) compliance using the Privacy Protected Display setting when adding the RDU node (see Step 17 of the procedure “Add a Node to the RoamAlert System” on page 4-13 for details).

The RDU uses a Molex connector plug and terminal block to connect power and network cabling and optional dry contact relays. See Table 3.7, “RDU Molex Connector Wiring” on page 53 for details.

An RDU package includes these components:

- 1 Remote Display Unit,
- 1 Cable assembly – 18” long,
- 8 insulated crimp connectors, and
- 1 mounting hardware pack with 4 nylon EZ drywall anchors and 4 screws.

For locally-connected RDUs, RJ-11 cable assemblies are available from Xmark.

RDU Installation Tips

- **Run power and network cables to each RDU location prior to installation.**
Leave at least 10 ft. (3 m) of slack, for location adjustment. Run power and RS-485 cables to the location.
- **Determine whether the RDU will terminate the RS-485 segment.**
If the RDU terminates an RS-485 segment, JP 101 on the RDU circuit board must be jumpered.
- **Determine whether the RDU will be locally-connected or not.**
If so, along with network and power connections, you will need an RJ-11 cable (available from Xmark) to connect the RDU to the KEYPAD jack on the controller.
- **Install and test the door controller before installing a locally-connected RDU.**
To correctly locate the RDU, the door controller’s exciter field limit should be known.
- **Locate locally-connected RDUs outside the door controller’s exciter field limit.**
RDUs being used as keypads should be located outside a controller’s exciter field limit, as an alarm cannot be cleared until the tag is removed from the field.
- **Attach the keypad cable before attaching the power cable to a locally-connected RDU.**
The RDU does not have an on-off switch. It automatically attempts to configure itself for local and remote functions as soon as power is supplied. If the RDU is not connected by keypad cable to the controller, local functions will not be configured.
- **Locate the RDU for easy access and viewing.**
The RDU should be mounted in an easily accessible location at an average viewing height (about 5’ / 1.52 meters). Avoid locations that are exposed to direct sunlight.

- **Power the RDU from the central power supply.**
The RDU requires 24VDC to operate. A locally-connected RDU can be powered by the controller if 100mA is available at the **+24VDC INPUT** pin. The amount of power available will depend on what other equipment may also be powered by the controller.
- **Determine whether the RDU and a keypad will be connected to the same controller.**
If a keypad and a locally-connected RDU will be connected to the same controller, contact Xmark technical support to obtain a custom splitter. The standard splitter supplied with the keypad will not work with an RDU.

RDU Installation Procedure

Follow these steps to install an RDU:

- 1 Record the RDU's serial number on the facility floor plan at the correct location. This serial number is required during software configuration to identify the unit. The serial number is found on the underside of the RDU beneath the bar code.
- 2 Remove the two screws on the bottom of the RDU and snap the case open. The rear panel of the RDU has a cut-out for cables and has multiple mounting holes for single and double-gang electrical boxes (#6-32 machine screws required) or for direct attachment to a wall (4 EZ drywall anchors and 4 screws supplied with unit).
- 3 Identify the location of the RDU, taking into consideration ease of access and viewing height, the presence of direct sunlight, and the limits of the exciter field (for locally-connected RDU).
- 4 Using the rear panel as a template, make a cut-out in the wall for cables, or if necessary, install a single or double-gang electrical box at the location.
- 5 Mount the RDU rear panel to the wall, making sure that it is level and securely attached.
- 6 Bring all cables to the cut-out, leaving enough slack to attach them to the RDU:
 - 6.1 Run the power cable from the CPS.
 - 6.2 Run the RS-485 cable from the previous device in the segment or from the controller.
 - 6.3 For a locally-connected RDU, run an RJ-11 cable from the controller's **KEYPAD** jack.
 - 6.4 For relay contacts, run the wiring from the relay.
- 7 On the cable assembly supplied with the RDU, strip the wiring, leaving approximately 3/8" bare. Be careful not to nick the copper.
- 8 Match the correct lead on the cable assembly to the lead from the RS-485, power, and if used, the relay wiring. See Table 3.7, "RDU Molex Connector Wiring" on page 53.
- 9 Insert both matching stripped leads into an insulated crimp connector (supplied) and crimp with pliers. Store any unused leads on the cable assembly out of the way.
- 10 If this is a locally-connected RDU, attach the RJ-11 cable from the controller's **KEYPAD** jack to the RJ-11 jack (**J201**) on the RDU PCB before attaching the cable assembly.
- 11 Defeat the tamper switch (**SW101**) at the upper left of the RDU PCB. This switch closes when the front panel is attached.
- 12 Attach the cable assembly to the Molex terminal block on the RDU PCB.
- 13 The RDU powers up and performs a self-test, then configures itself for remote functions and, if connected to a door controller, also configures itself for local functions.

Note: *Until the RDU has been added to the node list in the RoamAlert software, it displays the message "Host Communication Failed". This is normal.*
- 14 Hardware installation is complete. See the next section for setup and configuration.

RDU Configuration

Once installed, the RDU must be configured. Certain settings are made at the RDU itself, while other settings are made at the RoamAlert server PC.

At the RDU, you can:

- define speaker volume levels for Day and Night profiles and for Tamper conditions,
- define speaker tones for Day and Night profiles and for Tamper conditions,
- specify when the LCD backlight should remain on,
- reset the volume levels, tones, and backlight setting to the factory defaults, and
- view the RDU's firmware revision and serial number.

At the RoamAlert server PC, you can:

- add RDUs to the node list,
- place RDU icons on a floor plan, and
- define the time periods during each daily 24-hour cycle when RDUs use either the Day or Night profiles you have defined at each RDU.










In essence, each RDU can have its own volume level and tone settings for Day and Night profiles, but all RDUs have their Day or Night profiles activated during the same time periods.

Settings at the RoamAlert Server PC

- To add an RDU to the node list, refer to Step 17, page 4-16 of the “Add a Node to the RoamAlert System” procedure.
- To place RDU icons on a floor plan, refer to “Place a Node Icon on a Floor Plan” on page 4-27.
- To define the time periods during which an RDU uses its Day or Night profiles, refer to “Configure RDU Audible Alert Profiles” on page 4-12

Settings at the RDU

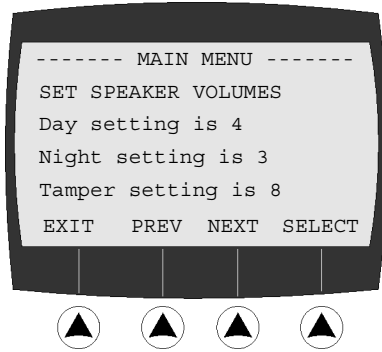
The RDU Main menu is accessed with a master password. The menu and option selection lists are displayed on the LCD screen and you use the buttons below the screen to select and set options. The labels at the bottom of the screen identify each button's usage during the operations you perform. The possible button functions are:

<u>EXIT</u>  Closes the Main menu	<u>PREV</u>  Goes to the previous screen in sequence	<u>NEXT</u>  Goes to the next screen in sequence	<u>SELECT</u>  Selects the current option	<u>CANCEL</u>  Returns to the previous screen without making any changes
<u>DOWN</u>  Selects the next item in a list or decreases a setting's value	<u>UP</u>  Selects the previous item in a list or increases a setting's value	<u>ACCEPT</u>  Accepts the current setting and goes back to the previous screen	<u>RESET</u>  Resets the RDU to factory default settings	> Used to indicate the selected option in a list

Accessing the RDU Main Menu

To access the Main menu, follow these steps:

- 1 Ensure that the RDU is powered up.
- 2 Enter **#090210#** at the RDU keypad. The # signs are part of the password and must be entered.
- 3 The RDU Main Menu is displayed at the Set Speaker Volumes page.

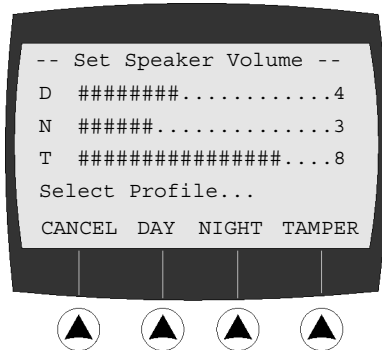


Note: If no buttons are pressed for 45 seconds, the RDU closes the menu and returns to its idle state. The password must be re-entered to access the menu again.

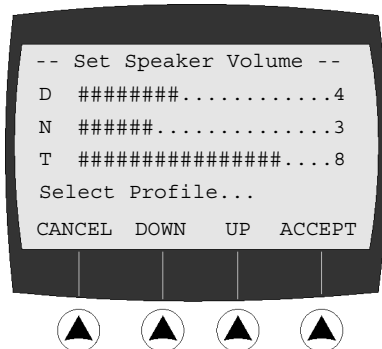
Setting the Speaker Volume Levels

To set the speaker volume levels for each profile, follow these steps:

- 1 At the Main Menu **SET SPEAKER VOLUMES** page, press the button under **SELECT**. The **Set speaker volumes** menu displays.



- 2 Press the button under the profile for which you want to set the volume, or press **CANCEL** to return to the Main menu **SET SPEAKER VOLUMES** page.

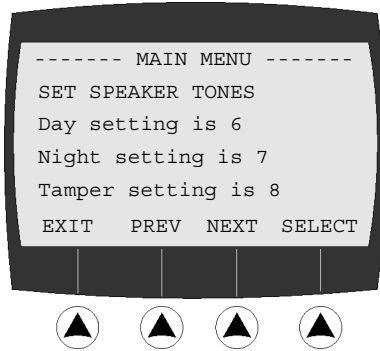


- 3 Press **DOWN** to decrease the volume or **UP** to increase the volume of the profile you selected. As you press the button, the speaker sounds at the selected volume and the value changes on the display. If you press **DOWN** until you reach **0**, the speaker is turned off.
Note: Do not set the speaker volume too low to be heard.
- 4 When you are satisfied with the volume setting, press **ACCEPT**. The volume setting is changed and you are returned to the screen where you can select another profile.
- 5 Repeat steps 2–4 to change the volume for the other profiles as necessary, then press **CANCEL** to return to the Main menu.

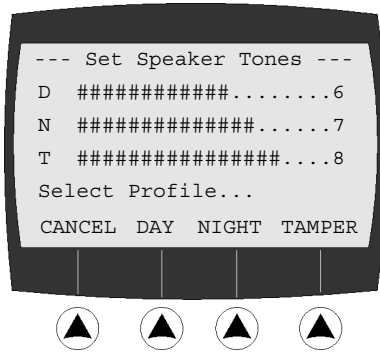
Setting the Speaker Tones

To set the speaker tones for each profile, follow these steps:

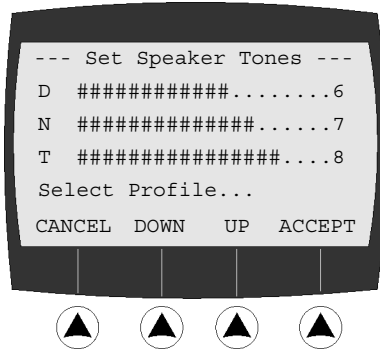
- 1 At the Main Menu **SET SPEAKER VOLUMES** page, press **NEXT** to go to the **SET SPEAKER TONES** page.



- 2 Press **SELECT**. The **Set Speaker Tones** menu displays.



- 3 Press the button under the profile for which you want to set the tone, or press **CANCEL** to return to the **SET SPEAKER TONES** page.

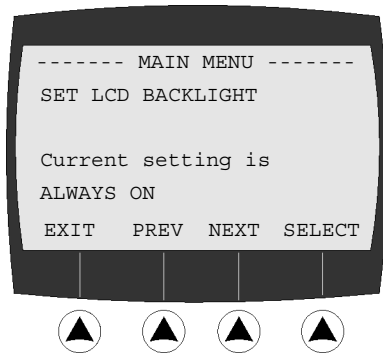


- 4 Press **DOWN** to lower the pitch of the tone or **UP** to raise the pitch of the tone for the profile you selected. As you press the button, the speaker sounds at the selected pitch and the value changes on the display. You can set nine different tones.
- 5 When you are satisfied with the tone setting, press **ACCEPT**. The tone setting is changed and you are returned to the screen where you can select another profile.
- 6 Repeat steps 3–5 to change the tone for the other profiles as necessary, then press **CANCEL** to return to the Main menu.

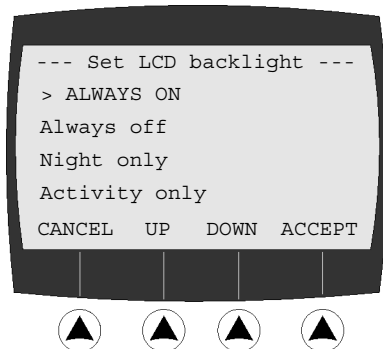
Setting the LCD Backlight

To set the LCD backlight, follow these steps:

- 1 At the Main Menu **SET SPEAKER VOLUMES** page, press **NEXT** twice to go to the **SET LCD BACKLIGHT** page.



- 2 Press **SELECT**. The **Set LCD backlight** menu displays. The **Always off** setting causes the backlight to remain off at all times. The **Night only** setting causes the backlight to turn on during Night profile time periods. The **Activity only** setting causes the backlight to turn on only when an alarm occurs or when a key is pressed on the keypad.

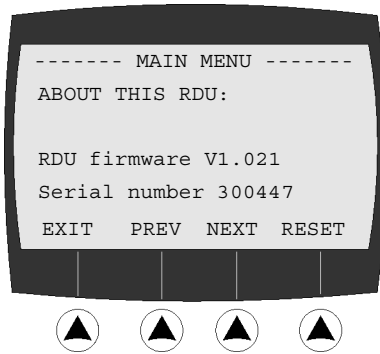


- 3 Press **DOWN** or **UP** to change the backlight setting, then press **ACCEPT** to save the setting and return to the **SET LCD BACKLIGHT** page.
- 4 Press **CANCEL** to return to the Main menu.

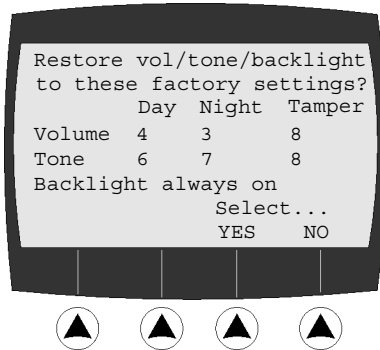
Viewing the Revision and Serial Number and Resetting the RDU

To view the revision and serial number or reset the RDU, follow these steps:

- 1 At the Main Menu **SET SPEAKER VOLUMES** page, press **NEXT** three times to go to the **ABOUT THIS RDU:** page.



- 2 To restore the RDU to its factory default settings, press **RESET**. The **Restore** page displays.



- 3 Press **YES** to restore the factory defaults shown and return to the **ABOUT THIS RDU:** page, or **NO** to cancel and return.

RDU Notes and Diagrams

Operating Modes

The RDU operates in one of these seven modes:

- **Idle Mode**
Initialization has completed successfully and there are no active alarms. The **POWER** LED is on.
- **Configuration Mode**
The master password has been entered and the menu is displayed. Volume, tone and backlight settings are made in this mode.
- **Remote or Local Alarm**
An alarm message from the server PC is displayed on the LCD screen, the **ALARM** LED is lit and the speaker sounds the tone.
- **Annotation Mode**
A subset of Local Alarm mode.
- **Bypass Mode**
A valid PIN number has been entered at the keypad. The **BYPASS** LED blinks.
- **Tamper Alarm**
The case of the RDU has been opened.

LED Display

The three LEDs on the RDU front panel display these indications:

LED	Color	Display	Indication
POWER	Amber	On	The RDU is receiving power
		Off	The RDU is not receiving power
BYPASS	Green and Red	Alternate blinking	Bypass mode, a valid PIN code has been entered
ALARM	Red	Short flashes	Pre-alarm (resident loitering near an exit)
		Long flashes	Full alarm, open door with a Tag in detection field

Audible Alarms

The RDU sounds alarms as follows:

Sound	Indication
Continuous beep	Tamper alarm, the RDU case has been opened
Long beeps	A tag is in the detection field of a locally-connected controller and the door is open
Pairs of beeps	A remote alarm has occurred
Short beeps	Local loiter alarm, a tag is in the detection field of a locally-connected controller but the door is closed

Note: Alarm details are not displayed on the LCD screen when the configuration menu is open.

RDU Communications with the RoamAlert Server

The RDU (or any other RoamAlert device) does not initiate communications with the server PC. The server PC polls each device in rapid and continuous sequence. The RDU reports its current status, which may include any of these conditions that might exist at the time it is polled:

- relay engaged (alarm),
- controller present (for locally-connected RDU),
- the current volume/tone/backlight configuration,
- the state of the tamper switch, and/or
- any PIN code that has been entered.

In response to this report, the server PC can command the RDU to:

- turn on the **ALARM** LED,
- sound an audible alarm,
- disable the RDU keypad, or
- change the profile to Day or Night (according to the time periods configured in software).

Molex Connector

The Molex connector plug is supplied with wiring as follows:

Table 3.7 RDU Molex Connector Wiring

MOLEX Pin	Cable Color	Connection	
		Local (on Controller)	Non-Local
1	Orange	Pin 1: +24VDC INPUT	24V DC
2	Black	Pin 4: SYSTEM GROUND	Ground
3	Red	Pin 5: RS-485 +	RS-485 +
4	Green	Pin 6: RS-485 –	RS-485 –
5	Black	Pin 7: SYSTEM GROUND	RS-485 Ground
6	Brown	Pin 16 or 19: COM 1 or COM 2	n/a
7	White	Pin 17 or 20: N.C. 1 or N.C. 2	n/a
8	Blue	Pin 15 or 18: N.O. 1 or N.O. 2	n/a

Cable Requirements

The RDU requires the following cables:

Table 3.8 RDU Cable Requirements

Purpose	Cable Required
Power (24VDC @ 100mA) Relay Contacts	<ul style="list-style-type: none"> Class 2 cable, or CU type CM or MP, or CSA type FT-4
RS-485 Network	Communication grade cable: <ul style="list-style-type: none"> max. 15pF per foot Impedance 120Ω
Local Controller	RJ-11 cable assembly, available from Xmark

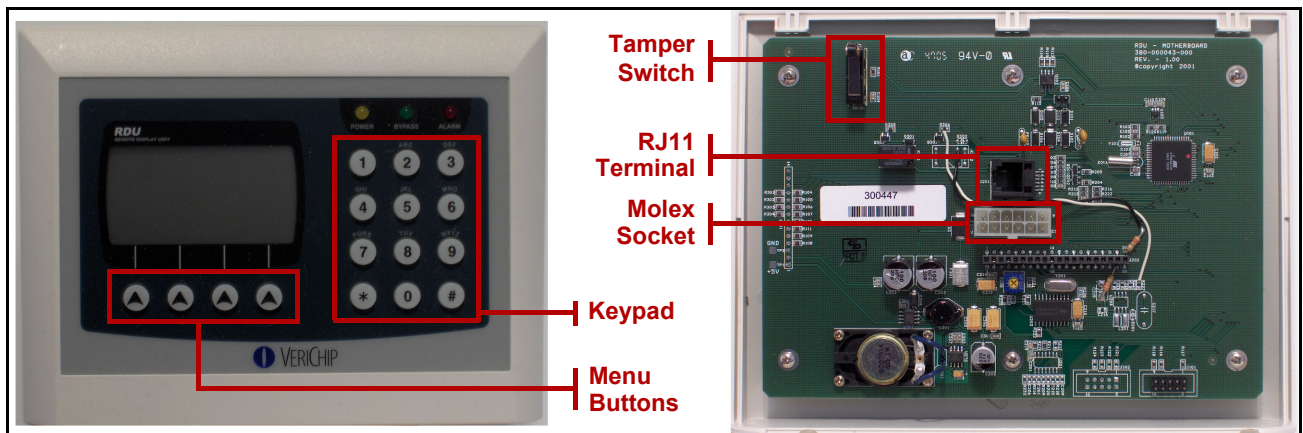


Figure 3-22: Remote Display Unit

Installing a Network Manager

The network manager is most useful in a large installation, particularly one that covers multiple floors. An NM can be positioned at each floor, connected through an existing Ethernet network to the RoamAlert server PC. This can greatly decrease the run length of the RS-485 network.

Technically, a network manager can control an RS-485 segment of up to 256 devices (controllers, receivers, I/O-8 modules). However, because of memory limitations, the number of devices is restricted by the software to 64.

If you are installing a RoamAlert Plug-in Server Bundle, the NM replaces the internal RS-485 card that used to be supplied. If you are installing a RoamAlert Self-Install Server Bundle, you replace the supplied external RS-232/485 converter with the NM.

Important: Network manager IP address configuration depends on the kind of Ethernet network being used to connect the NM with the RoamAlert server PC:

- **Corporate LAN (Local Area Network) with a DHCP server**
The NM must be set to obtain an IP address automatically.
- **Independent RoamAlert only Ethernet network (factory default)**
The NM must be given a static IP address. The factory setting is 192.168.0.146.

Network Manager Installation Tips

- **Run power and network cables to each network manager location prior to installation.**
Leave at least 10 ft. (3 m) of slack, for location adjustment. Run power, ethernet and RS-485 cables to the location.
- **Determine whether the NM will terminate the RS-485 segment.**
The RS-485 segment usually terminates at the NM and the built-in termination is enabled by default. However, if it is not appropriate to install the NM at the end of the segment, you can remove the termination jumpers from the NM's circuit board. See "Removing the Termination Jumpers" on page 3-55 for details.
- **Locate the NM for easy access and viewing.**
The Ethernet and RS-485 activity LEDs should be clearly visible. The NM may be placed on an appropriate surface or it may be wall-mounted in either of two orientations.
- **Power the NM from the central power supply.**
The NM requires 24VDC to operate.

Network Manager Installation Procedure

Follow these steps to install a network manager:

- 1 Connect the RS-485 cable:
 - Note:** *If it is absolutely necessary to use CAT-5e cable, it should be shielded.*
 - 1.1** Connect the positive wire to **RS-485 +** on the back of the NM.
 - 1.2** Connect the negative wire to **RS-485 -** on the back of the NM.
 - 1.3** Connect the ground wire to **GND** on the back of the NM.
- 2 Connect the Ethernet cable from the RoamAlert server PC (or the corporate network) to the **ETHERNET** jack on the back of the NM.
- 3 Connect the 24 VDC power cable (see Figure 3-25 on page 3-56):

- 3.1 Connect the red wire to **24 VDC +** on the NM back.
- 3.2 Connect the black wire to **24 VDC –** on the NM back.
- 4 Configure and test the NM. Refer to the **Network Manager Installation and Configuration Guide** for details.

Removing the Termination Jumpers

If the NM will not be the first or last device on an RS-485 segment, follow these steps to remove the termination jumpers:

- 1 Carefully remove the four rubber feet from the base of the NM to expose the case screws.
- 2 Remove the screws and lift the top off the unit.
- 3 Remove the three blue jumpers (**R215**, **R216**, and **R217**). See Figure 3-23 below.
- 4 Reassemble the unit.

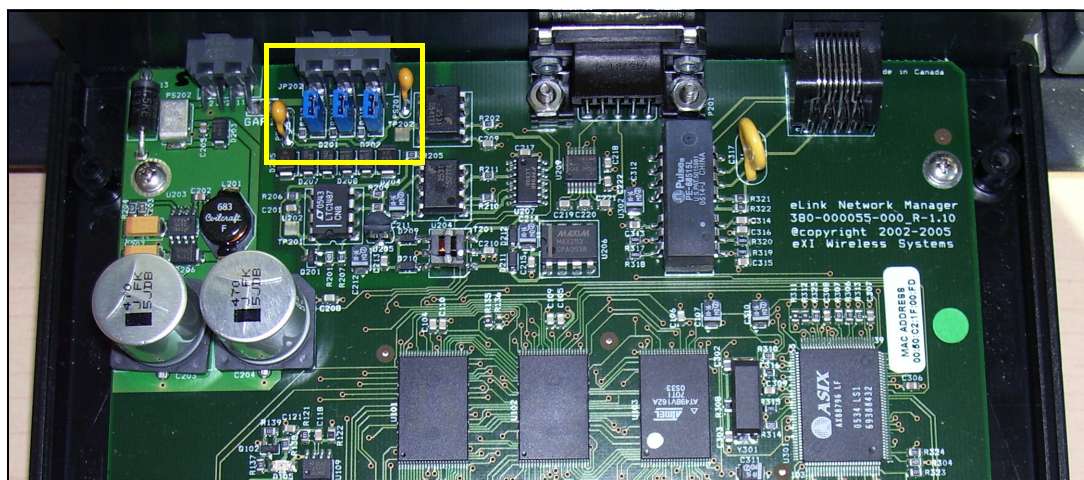


Figure 3-23: Network Manager Termination Jumpers

Network Manager Notes and Diagrams

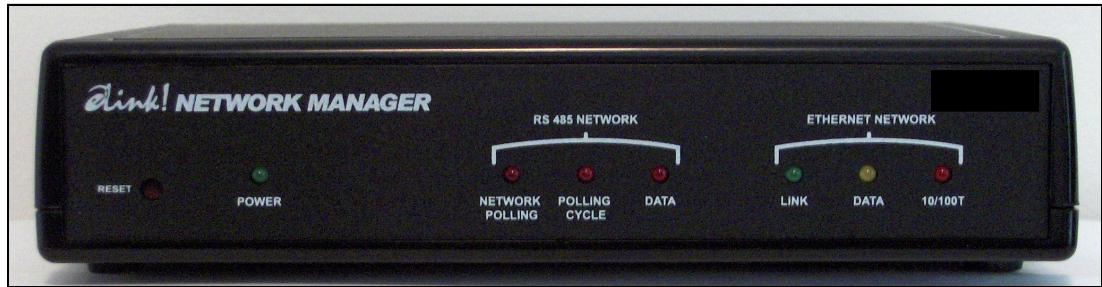


Figure 3-24: Network Manager Front View



Figure 3-25: Network Manager Back View

Chapter 4

SOFTWARE CONFIGURATION

This chapter describes the tasks required to configure the system for use. These tasks include:

- installing the RoamAlert software on the server and on consoles (if required),
- setting the RS-485 network communications port,
- setting global options,
- adding and configuring consoles (if required),
- adding and configuring nodes (controllers, receivers, I/O modules, RDUs) so that the software recognizes the devices in the system,
- adding floor plans and locating the server, consoles and nodes on those plans,
- adding users and assigning each an access level,
- adding tags to the tag database (inventory),
- adding and configuring tag categories,
- defining the annotations used when users accept alarms,
- configuring the sounds that are played when an alarm occurs,
- adding and configuring messaging devices (if used), and
- adding links (if I/O-8 modules are used).

When all devices have been installed and tested and the software has been configured, a final system check must be performed and the installed system must be documented before the system is turned over to the client. See the next chapter, System Commissioning, for details.

As you perform the configuration tasks, you record all details on the commissioning forms provided in Appendix A for that purpose. When completed, these forms will form part of the system documentation that you provide to the client at system commissioning.

Important: Print a copy of Form 1, “Software Configuration Checklist” before starting, and complete it as you work through the configuration tasks.

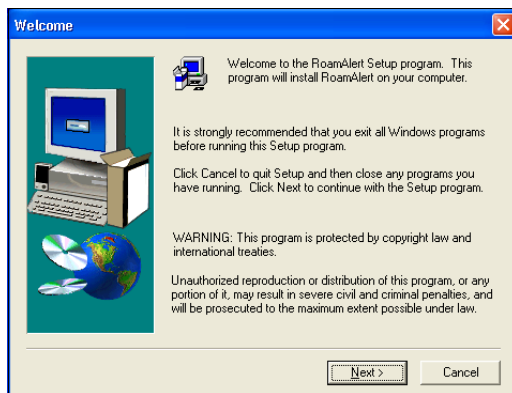
Installing the RoamAlert Software

The RoamAlert 4.3.1 software CD contains the following:

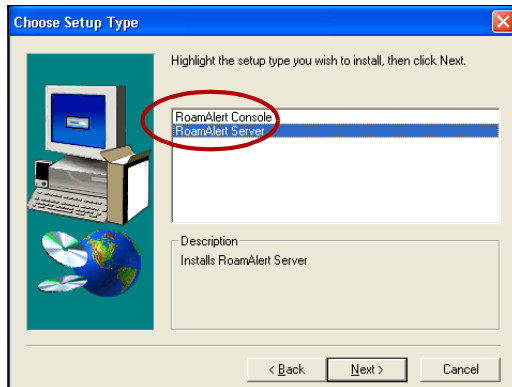
- Adobe Reader 7 software (for reading and printing all documentation),
- pocket tag reader software and documentation,
- tag link documentation,
- Xmark software license agreement,
- RoamAlert 4.3.1 software, and
- RoamAlert 4.3 system and installation documentation.

Procedure: To Install the RoamAlert Software on a Server or Client PC

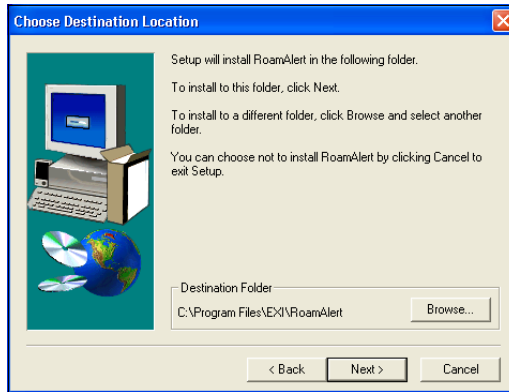
- 1 Insert the RoamAlert software CD into the CD drive of the server PC.
- 2 Make sure that you close all running programs before starting the installation.
- 3 At the Windows desktop, click **Start**, then **Run**.
- 4 **Browse** to the RoamAlert 1.2.10 folder on the CD and select the **Setup.exe** program.
- 5 Click **Open**, then **OK**. The RoamAlert setup program **Welcome** window opens.



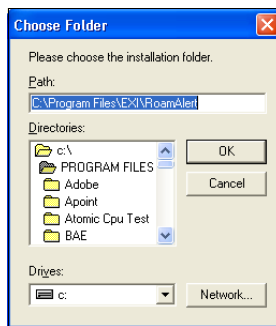
- 6 Click **Next**. The **Choose Setup Type** window opens.



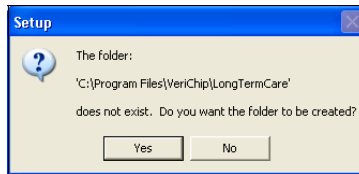
- 7 Select RoamAlert **Server**, then click **Next**. The **Choose Destination Location** window opens.



- 8 To accept the destination offered, click **Next**. Continue at Step 12.
- 9 To enter or choose another location, click **Browse**. The **Choose Folder** window opens.

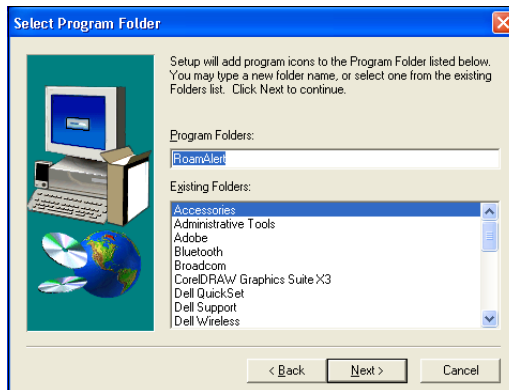


- 10 Select an installation folder from the **Drives** and **Directories** boxes, or type a new folder name in the **Path** box, then click **OK**.
- 11 If you enter a folder that does not exist, you are asked to confirm its creation:



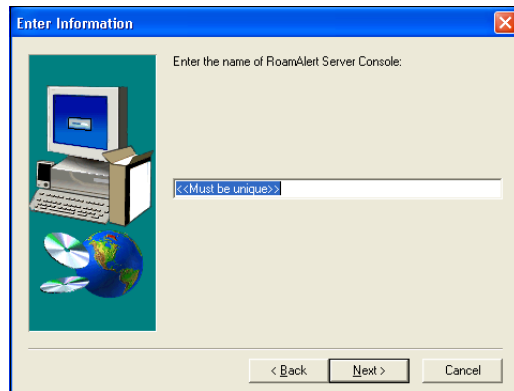
Click **Yes** to create the new folder.

- 12 The **Select Program Folder** window opens.

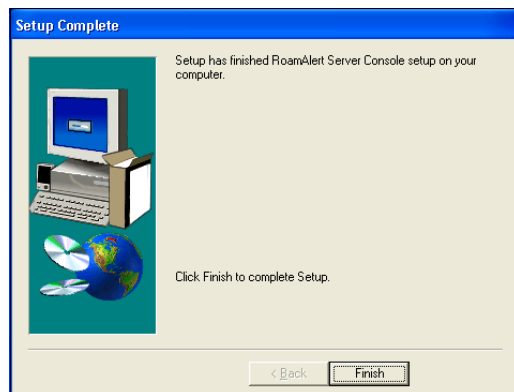


This is the folder on the Windows Start menu to which RoamAlert software program icons will be added.

- 13 Select an existing folder or type a new name, then click **Next**. The **Enter Information** window opens.



- 14 Each RoamAlert server and console must have a different name. Enter a unique name for this computer, then click **Next**. The **Setup Complete** window opens.



- 15 Click **Finish** to complete the setup procedure.
- 16 Repeat this procedure for each console in the system.

Important: For consoles, select RoamAlert **Console** in Step 7.

Procedure: To Test the RoamAlert Software Installation

- 1 When the installation is complete, verify that the program starts:
 - double-click the RoamAlert icon on the desktop, or
 - select **Programs > RoamAlert > RoamAlert** from the **Start** menu.
- 2 After a moment or two, the RoamAlert main window should appear. To exit:
 - click the red **Close** box at the upper right of the window, or
 - press **Alt-Q** on the keyboard, then
 - enter your **User Name** and **Password**, and click **OK**.

Note: During installation, RoamAlert places a shortcut in the folder:

`C:\Documents and Settings\All Users\Start Menu\Programs\Startup`

If you do not want RoamAlert to start each time this computer is turned on, navigate to that folder and delete the shortcut.

System Access Levels

Before you configure RoamAlert, you need to understand user modes and system access levels.

There are four modes by which authorized users gain access to the different RoamAlert functions:

- User,
- Supervisor, and
- Administrator.

RoamAlert is pre-configured with one Administrator user account called **sa**. An Administrator is the only user type with access to all RoamAlert functions.

To switch between modes:

- Press **Alt** and **L** to access the Supervisor level.
- Press **Alt** and **D** to access the Administrator level.
- Press **Alt** and **U** to return to the User level.

A User can assign tags to residents and discharge residents, accept alarms and locate tags within the protected area. A Team Leader works at the User level, but can also disable and transport tags. Supervisors and Administrators manage the system. Refer to the RoamAlert System Manual for a complete list of the RoamAlert functions available in each mode.

Configuring RoamAlert Software

Following installation on the server and any consoles, the RoamAlert software must be configured. Software configuration is performed at the RoamAlert server PC. The console PCs are updated automatically as changes are made at the server.

Certain tasks must be performed in sequence. For example, consoles cannot be configured until nodes have been added, nodes cannot be placed on floor plans until the nodes are configured, messaging devices cannot be added until consoles are configured, and links cannot be defined until I/O-8 modules are added.

Configuring the RoamAlert software in the following specific order will ensure that all dependencies are addressed:

- 1 Log in to Administrator Mode.
- 2 Set global configuration options.
- 3 If Network Managers are being used, a license must be issued that specifies Network Manager use, accompanied by a **Client Application ID**. This ID must be specified using the Network Manager configuration software. See the **Initial Configuration** section of the **Network Manager Installation and Configuration Guide** (part # **980-000022-000 R2.0**) for details.
- 4 Add and configure nodes (controllers, receivers, I/O-8 modules).
- 5 Change the RS-485 network communications port (only if you cannot add the first node).
- 6 Add and configure consoles (if required).
- 7 Add floor plans.
- 8 Place nodes (and consoles) on the floor plans.
- 9 Add users and set their access levels.
- 10 Add tags to the tag database (inventory).
- 11 Add tag categories,
- 12 Add annotations for alarm acceptance procedures.
- 13 Add and configure alarm notification sounds.
- 14 Add and configure messaging devices (if used), and
- 15 Add links (if I/O-8 modules are used).

Important: *All tasks must be performed at the RoamAlert server PC.*

To configure the RoamAlert software, you must be logged into Administrator Mode so that you have access to all software functions.

Procedure: To Log Into Administrator Mode at the Server PC



- 1 At the keyboard of the server PC, press the **Alt** and **D** keys simultaneously. The **Administrator Login** dialog box opens.

Note: *All communication with the console PCs is suspended while the server PC is in Administrator mode.*



Note: At the right a vertical timer counts off the seconds. If you do not complete the logon procedure within 1 minute, the dialog box closes and you must start again.

- 2 Type in your User Name, then press **Tab** or **Enter**.
- 3 Type in your Password. The **OK** button is now enabled.
- 4 Click **OK** or press **Enter**. RoamAlert switches to Administrator mode.

Note: All tasks in this Configuration section assume that you are logged into Administrator mode at the RoamAlert server PC.

Change the RS-485 Network Port

Important: If the Network Manager is being used, skip this section and do NOT alter any settings in the RS-485 Network window.

During software installation, RoamAlert automatically adds the RS-485 network to the system and configures its communications port and baud rate.

There may be installations, however, where RoamAlert does not correctly ascertain the port for a server PC. In this situation, RoamAlert will issue a **Node not found** error when you attempt to add and configure the first node in the system.

Since the RS-485 communications port can only be specified when adding an RS-485 network, you need to perform these tasks to correct the problem.

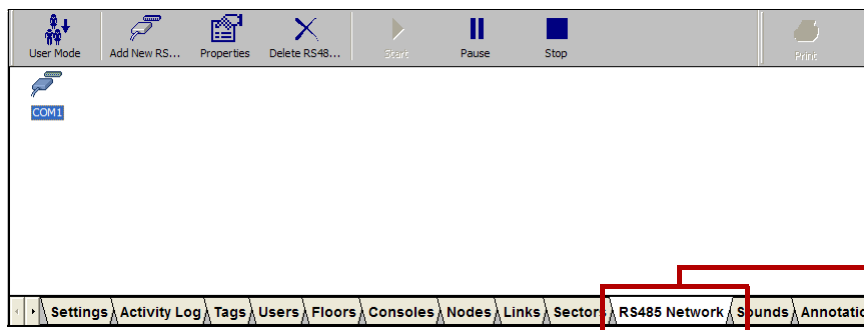
- delete the RS-485 network from the software,
- add a new RS-485 network, and then exit and restart RoamAlert.

These tasks are described below.

Procedure: Delete the RS-485 Network



- 1 At the RoamAlert server in Administrator mode, select the **RS-485 Network** tab.



- 2 Click the network icon to highlight it.



- 3 Click **Delete RS-485 Network** on the toolbar. The **Delete RS-485 Network Wizard** opens.



- 4 Review the information to ensure that this is the network you wish to delete.
- 5 Click **Cancel** to keep the network and return to the RS-485 Network panel, or click **Finish** to delete the network and return to the RS-485 Network panel.

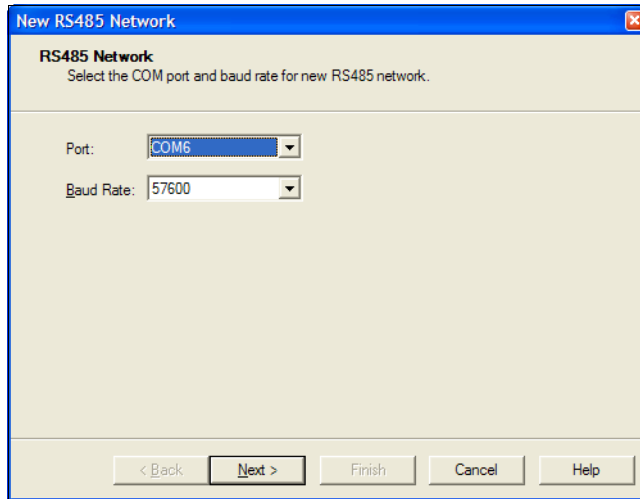
Procedure: Add the New RS-485 Network



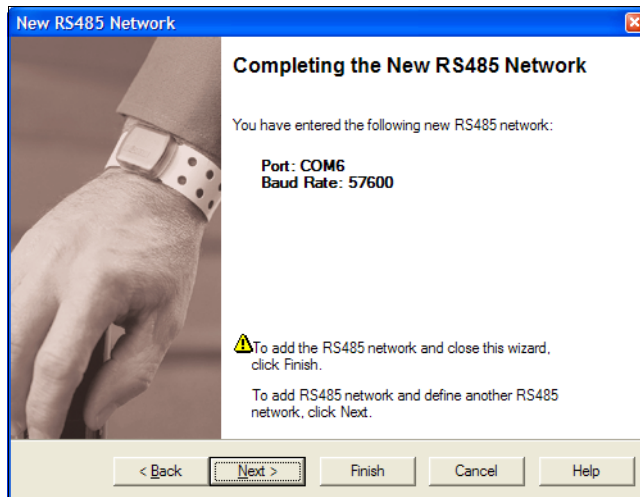
- 1 Click **Add New RS-485 Network** on the toolbar. The **New RS-485 Network Wizard** window opens.



- 2 Click **Next** to continue to the **RS-485 Network** window. The next available COM port and the default baud rate of 57,600 are pre-selected. Unless specifically directed by Xmark, do not change the baud rate.



- 3 Select the correct communications port, then click **Next** to continue to the **Completing the New RS-485 Network** window.



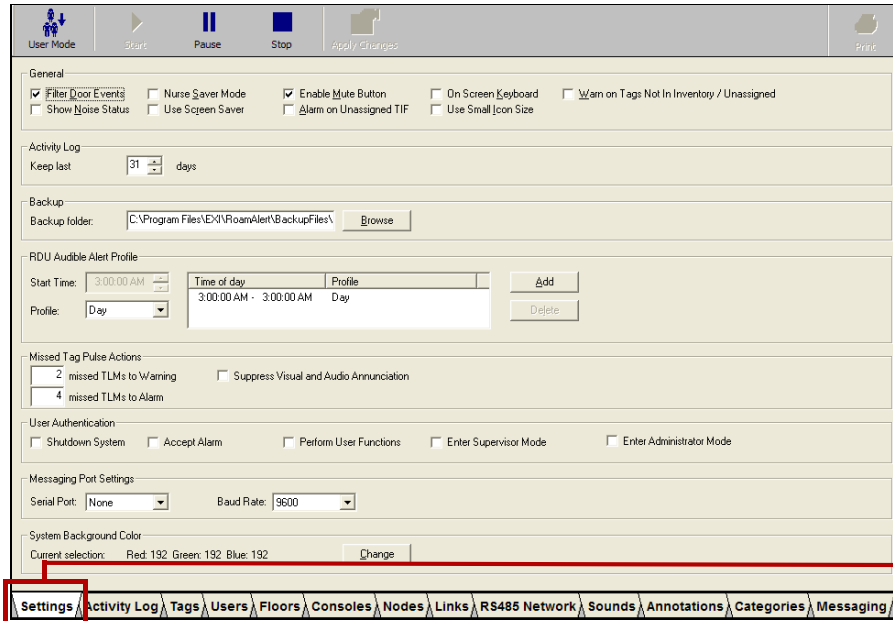
- 4 Review the information for this new network. If the port or baud rate is not correct:
 - click **Back** to make changes, or
 - click **Cancel** to close the Wizard without adding the network.
 If you are satisfied with the displayed information:
 - click **Finish** to add this new network and close the New RS-485 Network Wizard, or
 - click **Next** to add this network and begin adding another network.
 The new network is added to the RS-485 Network panel.
- 5 To exit and restart RoamAlert,
 - 5.1 click the red **Close** box at the upper right of the window, or press **Alt-Q** on the keyboard, then
 - 5.2 enter your **User Name** and **Password**, and click **OK**.
 - 5.3 Restart the RoamAlert application from the desktop.

Set Global Configuration Options

You must configure the RoamAlert software to meet the specific needs of the installation. The options configured here will have been assessed during consultations with the client.

Procedure: Set Global Configuration Options at the Server PC

- 1 Make a photocopy of **Form 2** to record the settings. In the **Setting** column, record the entries you make for each setting. In the column, mark off each setting as you complete it.
- 2 At the RoamAlert server PC, log in to Administrator mode and select the **Settings** tab if necessary. The Settings panel opens.



Warning

The **Start**, **Pause** and **Stop** buttons on the toolbar are used by VeriChip technical personnel to troubleshoot and perform maintenance. Clicking one of these buttons disables the system.

- 3 Adjust the settings as required. A checkmark in the setting's option box enables the setting, removing the checkmark disables the setting. Table 4.1 (starting on the next page) describes the usage of each setting in detail.
- 4 To apply (save) your adjustments while remaining at the Settings panel, click the **Apply Changes** button. To leave the Settings panel, click another tab or the **User Mode** button (your changes are also saved).

Table 4.1 RoamAlert Configuration Settings

Setting	Usage
General	
Filter Door Events	The system ignores all door open and close activities and does not add them to the Activity Log. This setting is recommended, as it helps keep the log manageable, particularly in a facility with elevators.
Show Noise Status	An overlay warning icon is displayed on the floor plan at the node experiencing extraneous RF noise. This warning may indicate that the node is not operating properly. Usually used when troubleshooting.

Table 4.1 RoamAlert Configuration Settings (continued)

Setting	Usage
Nurse Saver Mode	A wrist tag near a closed door gives a local alarm at the keypad only. Otherwise, a full alarm is given when a tag is near a closed door. <ul style="list-style-type: none"> a Tag near an open door always triggers a full alarm.
Use Screen Saver	Activates a screen saver on any console PC following 5 minutes of inactivity. The screen saver is cancelled when an alarm is received or an activity is performed at the console PC.
Enable Mute Button	Allows any user to silence an alarm before accepting it. Otherwise the mute button is unavailable.
Alarm on Unassigned TIF	An unassigned tag (in tag database but not admitted) triggers an exit alarm (Tag in Field) when detected at an exit. Helps prevent loss of tags.
On Screen Keyboard	Users can display an on-screen keyboard for data entry. (On-screen keyboard software must be installed to use this feature.)
Use Small Icon Size	Floor Plan icons are displayed at a reduced size. Useful if a floor plan is crowded with icons.
Warn on Tags Not In Inventory/Unassigned	A tag not in inventory (not added to the tag database) or unassigned triggers warnings and alarms.
Activity Log	
Keep Last nn Days	Use the arrows or type a value from 1 to 999 to specify the number of days to keep logs in the Activity Log list. After this period, the oldest log entries are discarded. A manual backup should be performed at the end of each period to keep logs on file.
Backup	
Backup Folder	If you wish to change the configured default backup location, use the Browse button to select an alternate disk/folder in which to store RoamAlert backup files.
RDU Audible Alert Profile	If you are installing RDUs (Remote Display Units) at this facility see "Configuring RDU Audible Alert Profiles" on page 4-12 for details.
Missed Tag Pulse Actions	
nn missed TLMs to Warning	In the box, type the number of missed Tag Pulses (TLM) before a warning is triggered. The value can be from 1 - 20, the default is 2. A typical optimal setting is 4.
nn missed TLMs to Alarm	In the box, type the number of missed Tag Pulses before an alarm is triggered. The value can be from 1 - 20, the default is 4. A typical optimal setting is 8. <p>Notes:</p> <ul style="list-style-type: none"> This value should be higher than the warning value to avoid receiving alarms before warnings. Wrist tag pulses occur at 16-second intervals.
Suppress Visual and Audio Annunciation	Prevents the visual display, audio and logging of missed TLMs.
User Authentication	
Shutdown System Accept Alarm Perform User Functions Enter Supervisor Mode Enter Administrator Mode	Enable or disable user login for each function. Authentication should always be enabled.

Table 4.1 RoamAlert Configuration Settings (continued)

Setting	Usage
Messaging Port Settings	
Serial Port	If your facility has a paging interface (Messaging), this setting identifies the serial port used by the interface. Messages are sent out the selected port using the TAP protocol, which is 7 bits, even parity, one stop bit (7E1).
Baud Rate	If your facility has a paging interface (Messaging), use this setting to select the appropriate baud rate for the interface.
System Background Color	
Change Current Selection	Click the Change button to select a different background color for the system background.

Configuring RDU Audible Alert Profiles

An RDU (Remote Display Unit) is a compact unit that combines a keypad with a small screen and speaker. The screen and speaker display and sound alarms. From the keypad, you can accept alarms at the RDU without returning to a console or the server. If it is connected to a door controller, the RDU also acts as a standard access keypad.

The speaker volume of an RDU can be set to 9 loudness levels, from completely off (0) to loud (8). When the RDU is installed, two separate loudness levels are configured for the speaker volume, one for daytime and one for night. Depending on the location of the RDU, the day profile may be configured at a high loudness level, and the night profile configured at a very low loudness level.

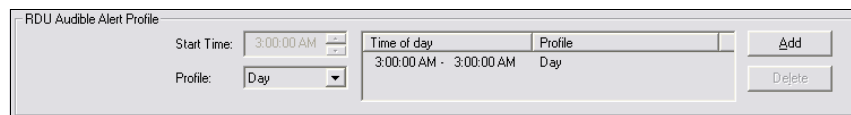
You can set up to eight time periods during a 24-hour day and define them as either day or night periods. At the starting time for each of these time periods, RoamAlert signals all RDUs to switch to the profile defined for that period.

Procedure: Configure RDU Audible Alert Profiles



- 1 At the RoamAlert server, log in to Administrator mode and select the **Settings** tab if necessary. The Settings panel opens.

In the **RDU Audible Alert Profile** section, the first of the eight possible time periods is defined by default to cover the entire 24-hour day and is set to the Day profile.



- 2 Click **Add** to create a second time period.
- 3 Select the time period you just added. The **Start Time** box becomes available.
- 4 Click the hour, minutes, or seconds and use the arrows to increase or decrease the Start Time value. As you do, RoamAlert adjusts the end and start times for the previous time period.
- 5 Click the arrow in the **Profile** box to select Day or Night for this period.
- 6 Repeat Steps 2 to 5 for up to 6 other time periods.

Add and Configure Nodes

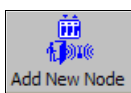
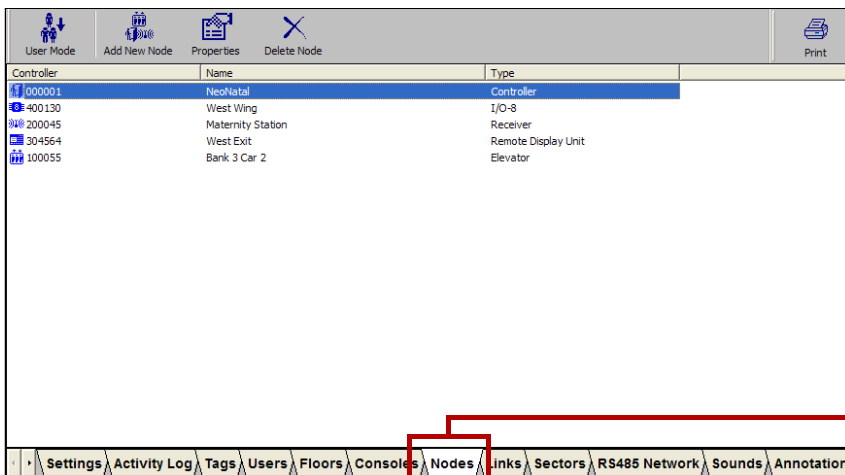
Each node that you have installed (door and elevator controllers, receivers, I/O-8 modules, RDUs) must be added to the system before it can be recognized by the RoamAlert software.

Procedure: Add a Node to the RoamAlert System

- 1 For every four (4) door controllers that you are adding, make one photocopy of **Form 3**.
- 2 For every six (6) elevator controllers that you are adding, make one photocopy of **Form 3**.
- 3 For every six (6) receivers that you are adding, make one photocopy of **Form 3**.
- 4 For each I/O-8 module that you are adding, make one photocopy of **Form 6**.
- 5 For each RDU that you are adding, make one photocopy of **Form 6**.
- 6 In the **Setting** column of each form, record the entries you make for each setting. In the **✓** column, mark off each setting as you complete it.



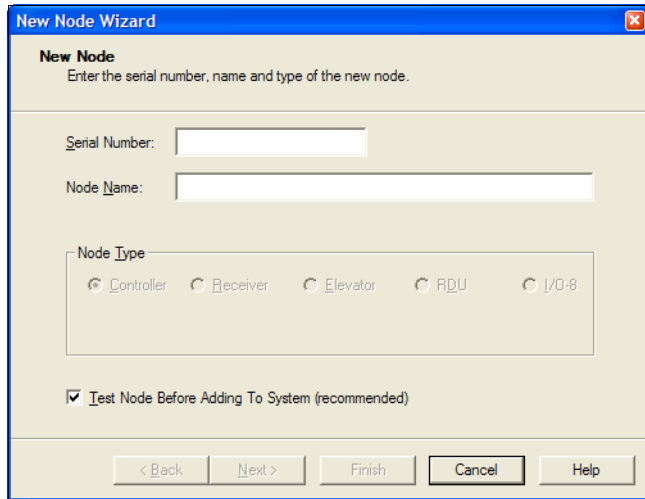
- 7 At the RoamAlert server in Administrator mode, select the **Nodes** tab.



- 8 Click **Add New Node** on the toolbar. The **New Node Wizard** window opens.



- 9 Click **Next** to continue to the **New Node** window.



- 10 Enter the **Serial Number** for the node. As you type the first digit, RoamAlert enables one or more **Node Type** options.
- 11 Type in a **Node Name** for this new node. Provide a name that clearly reflects the location of the node. For example, a receiver in a resident room might be called **Room 204**, or a door controller might be called **West Stairway**.
- 12 Make sure to select the correct **Node Type**.
- 13 Make sure that **Test Node Before Adding To System** is checked. This will ensure that the node is communicating with the server PC.
- 14 Click **Next** and, according to the node type you selected, continue configuration as follows:

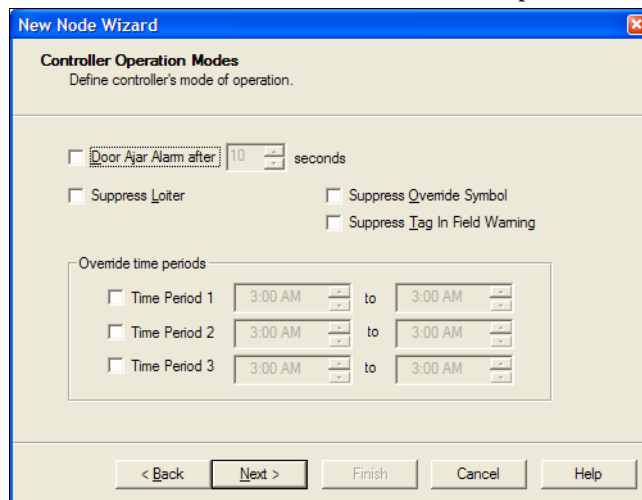


- For receivers or for elevator controllers, there is no further configuration. The **Completing the New Node Wizard** window opens. Go to Step 18.
- For door controllers, continue at Step 15.
- For I/O-8 modules, continue at Step 16.
- For RDUs, continue at Step 17.



- 15 Configuring the door controller:

15.1 The **Controller Operation Modes** window opens.

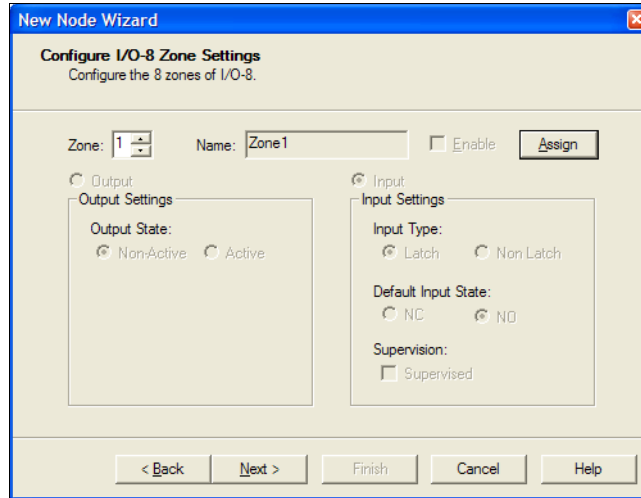


- 15.2 To set a **Door Ajar Alarm**, select the check box and use the arrows to select, in 1 second increments, the length of time after which a door left ajar will activate the alarm.
- 15.3 To prevent this controller from issuing loiter alarms, click the **Suppress Loiter** check box.
- 15.4 Click **Next** to continue to the **Completing the New Node Wizard** window. Go to Step 18.

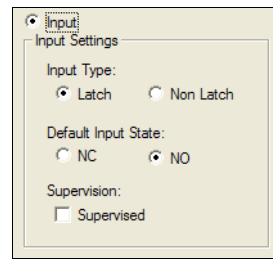
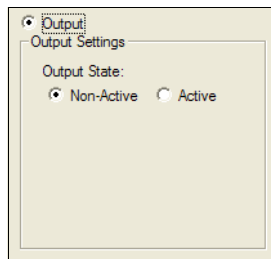


16 Configuring the I/O-8 module:

- 16.1 The **Configure I/O-8 Zone Settings** window opens. Up to 8 zones can be assigned to an I/O-8 module. Each zone can be either an output or an input zone.



- 16.2 Use the up and down arrows to select a zone number (1-8) from the **Zone** box, then click **Assign**.
- Note:** *If the zone you select has already been assigned, the Assign button is labelled **Unassign**.*
- 16.3 Type in a logical **Name** for this zone, for example **Corridor 3**.
- 16.4 Click the **Enable** check box to activate this zone immediately upon completion of the New Node wizard. You can enable the zone later by editing its properties.
- 16.5 Select either **Output** or **Input** to activate the appropriate option group for the zone.



- 16.6 Select the **Output** or **Input** options as follows:

Output State	Non-Active	The output is normally OFF.
	Active	The output is normally ON.

Input Type	Latch	The host controller will report an alarm when the zone is in alarm (i.e., not in the default state), and will continue to repeat the alarm until the zone input returns to the normal/default state and the user accepts the alarm.
	Non-Latch	The host controller will report the alarm as long as the zone is in alarm and will automatically acknowledge the alarm when the input condition returns to normal/default state.
Default Input NC State	Normally Closed	Normally Closed – zone contact is closed and an alarm is generated when the zone contact opens.
	NO	Normally Open – zone contact is open and an alarm is generated when the zone contact closes.
Supervision	Depending on whether an end-of-line termination resistor is installed at the input zone, it can be categorized as a Supervised zone or Non-Supervised zone. Configuring the input zone as a Supervised zone will help to detect whether the input switch is being tampered with, i.e. if the switch is hard-wired or open circuited. Normally open contacts require an end-of-line termination resistor in parallel with the switch contacts for Supervised operation. Normally closed contacts require an end-of-line termination resistor in series with the switch contacts for Supervised operation.	

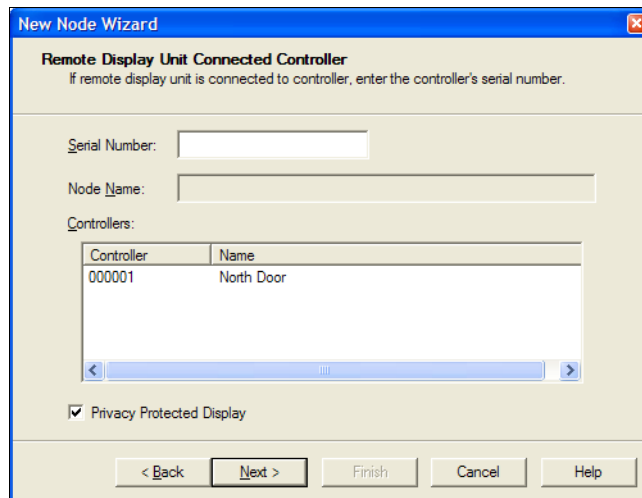
16.7 Repeat Steps 16.2 to 16.6 for each zone you are configuring for this module.

16.8 Click **Next** to continue to the **Completing the New Node Wizard** window.



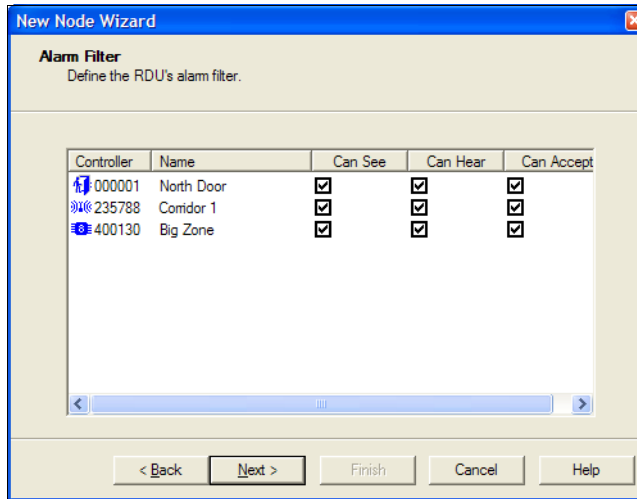
17 Configuring the RDU:

17.1 The **Remote Display Unit Connected Controller** window opens. An RDU can be connected to the network only or it can be connected to a specific controller as well as to the network.



17.2 If this RDU is connected to a controller, type in the **Serial Number** of the controller or select the controller from the list.

17.3 Check off **Privacy Protected Display** to ensure that the RDU is HIPAA compliant where required by law. Click **Next** to continue to the **Alarm Filter** window.



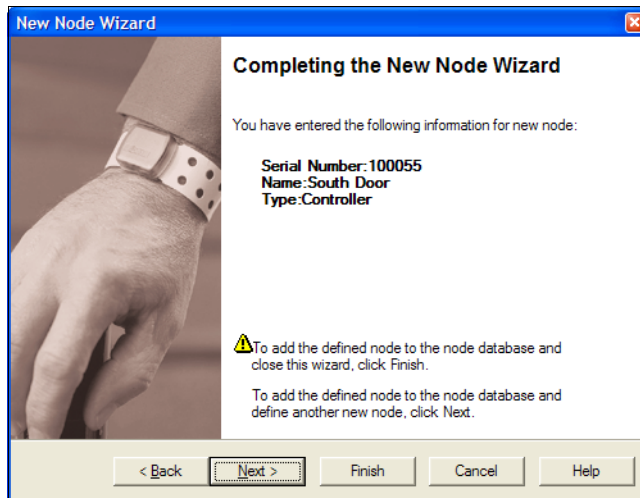
17.4 A node list is displayed with check boxes for each alarm filter setting. By default, an RDU can see, hear, and accept alarms from all door and elevator controllers, receivers, and I/O-8 modules in the RoamAlert system. For each node listed in the **Controller** column, select the filter settings for this RDU:

- **Can See** – this RDU displays alarms on the floor plan,
- **Can Hear** – this RDU sounds alarms on its speaker,
- **Can Accept** – this RDU can accept alarms.


Uncheck **Can See** to prevent this RDU from receiving alarms from that specific node.

17.5 Click **Next** to continue to the **Completing the New Node Wizard** window.

18 In the **Completing the New Node Wizard** window, review the information you entered for this new node.



- click **Back** to make changes, or
 - click **Cancel** to close the Wizard without adding the node.
- If you are satisfied with the displayed information:
- click **Next** to add this node and begin adding another node, or
 - click **Finish** to add this new node and close the New Node Wizard.
- The new node is added to the Node List.

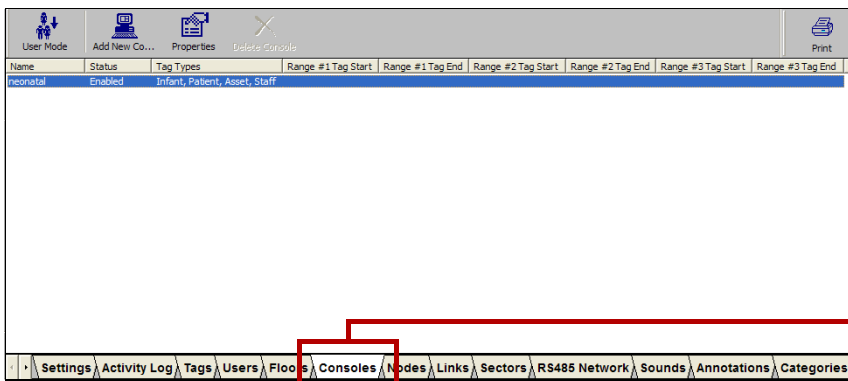
Important: If the message:  **Node not found** appears when you click **Next** or **Finish** while adding the **first** node to the system, two possible errors may have occurred. Either the node is not properly connected to the system or the RS-485 Network communication port is not set correctly. If the problem is with the RS-485 port setting, refer to the section “Change the RS-485 Network Port” on page 4-7 for details.

Add and Configure Consoles

When the RoamAlert software is installed, the server PC is added automatically. In this section, you will add and configure any console PCs, and adjust the configuration of the server PC if necessary.

Procedure: To Add a Console to the RoamAlert System

- 1 For each console that you are adding, make one photocopy of **Form 6**.
- 2 In the **Setting** column of each form, record the entries you make for each setting. In the column, mark off each setting as you complete it.
- 3 At the RoamAlert server in Administrator mode, select the **Consoles** tab.



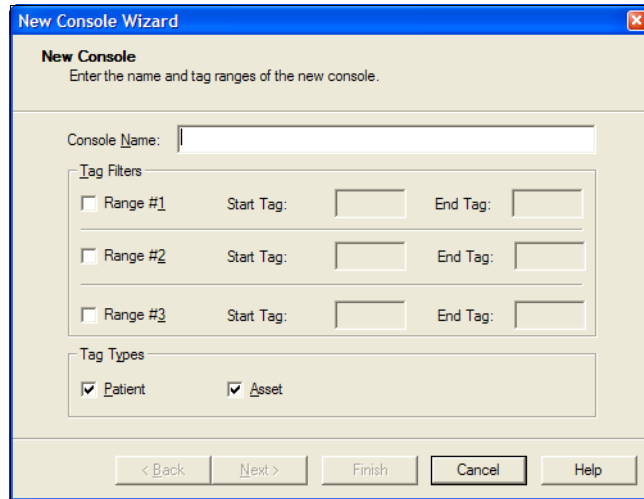
Consoles
Tab



- 4 Click **Add New Console** on the toolbar. The **New Console Wizard** window opens.



- 5 Click **Next** to continue to the **New Console** window.

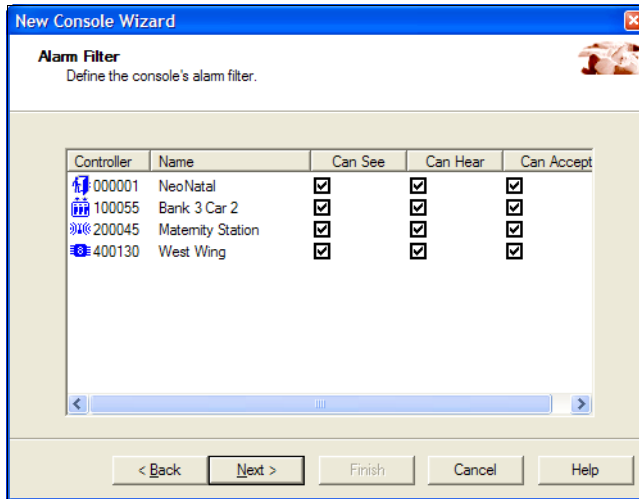


- 6 Fill in the information for this new console PC as follows:

Console Name	The name must be unique and should be an easily recognizable description of the console PC (usually its location) e.g. Nursery
Tag Filters	Specify up to 3 tag ID ranges for which alarms will be received by this console PC, all others are ignored. Leave these filters blank to receive alarms from all tags.
Tag Types	Check the tag types for which this console PC will receive alarms. Uncheck the tag types to be ignored.
Suppress Missed Tag Pulse...	Select this option to have this console PC ignore all TLM (Tag Location Messages). The server PC still records TLMs in the Activity Log.
Startup Mode Select	<p>Selecting Normal Mode allows other Windows applications to run concurrently with RoamAlert on this console PC. RoamAlert can be minimized at any time, but alarms or warnings automatically maximize the RoamAlert window.</p> <p>Selecting Secure Mode prevents the RoamAlert application from being minimized on this console PC. No other application can be run concurrently.</p> <p>Note: <i>Making a selection here requires a restart of RoamAlert on this console/server.</i></p>

The **Next** button is enabled when the **Name** field is filled.

- 7 Click **Next** to continue to the **Alarm Filter** window. A node list is displayed with check boxes for each alarm filter setting. By default, the console PC can see, hear, and accept alarms from all door and elevator controllers, receivers, and I/O-8 modules in the RoamAlert system.



For each node listed in the **Controller** column, select the filter settings for this console PC:

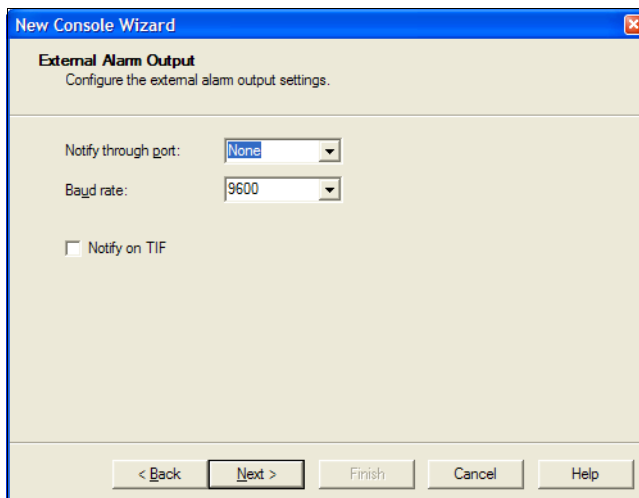
- **Can See** – this console PC displays alarms on the floor plan,
- **Can Hear** – this console PC sounds alarms on its speaker,
- **Can Accept** – this console PC can accept alarms.

Uncheck **Can See** to prevent this console PC from receiving alarms from that specific node.

Note: *Alarm Filter settings for this console PC take precedence over the **Multi Floor TIC discrimination** setting in the Settings panel. That is, if so configured, this console PC will see the alarms from a controller on another floor, even if Multi Floor TIC Discrimination is turned on.*

8 Click **Next** to continue to the **External Alarm Output** window.

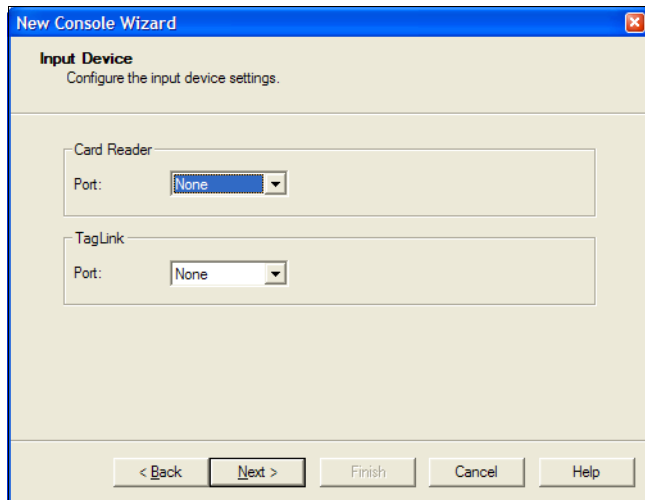
In the previous step, you identified the controllers from which this console PC can receive alarms. In this step, you define whether or not this console PC can pass these alarms on to external equipment through an alarm output module that is physically connected to the console PC.



9 Fill in the information for alarm output as follows:

Notify through port	If an alarm output module is connected to this console PC, select the COM port number for the module. Leave at None if no module is connected to this console PC.
Baud rate	From the drop-down list, select the baud (bits per second) rate for the port.
Notify on TIC	Select this box to send notifications for Tag Initiated Communications (off-body alarms)
Notify on TIF	Select this box to send notifications for Tag In Field messages (exit alarms)

10 Click **Next** to continue to the **Input Device** window.



11 If a card reader or a Tag Link is connected to this console PC, select the COM port that the device is connected to. (You may need to refer to the device settings in the Windows Control Panel to retrieve these port numbers.)

12 Click **Next** to continue to the **Completing the New Console Wizard** window.



13 Review the name and tag ranges (if specified) you entered for this console PC.

If you are not satisfied, click **Back** to make changes, or click **Cancel** to close the wizard without adding the console PC.

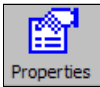
If you are satisfied, click **Next** to save the console PC and start adding another, or click **Finish** to save the console PC and close the wizard.

The new console PC is added to the console PC list.

- 14 Repeat this procedure for each console PC in the system.

Procedure: To Adjust the Configuration of the Server PC (or any console)

- 1 For the server, make one photocopy of **Form 6**.
- 2 In the **Setting** column of the form, record the entries you make for each setting. In the ✓ column, mark off each setting as you complete it.
- 3 In the Consoles list, double-click the server PC, or select the server and click **Properties** on the toolbar. The **Console Properties sheet** opens at the General panel. Open each property panel as needed to make changes (see “To Add a Console to the RoamAlert System” for field details).



Console Properties dialog, General tab. Name: RoamServer. Status: Enabled. Tag Ranges: Range #1, #2, #3. Tag Types: Patient, Asset.

Console Properties dialog, External Alarm Output tab. Table with columns: Controller, Name, Can See, Can Hear.

Controller	Name	Can See	Can Hear
000001	North Door	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
235788	Corridor 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
400130	Big Zone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Console Properties dialog, Input Device tab. Notify through port: None. Baud rate: 9600. Notify on TIF: .

Console Properties dialog, Alarm Filter tab. Card Reader Port: None. TagLink Port: COM8.

- 4 To close the properties sheet without saving your changes, click **Cancel**. To save your changes and close the properties sheet, click **OK**.

Add Floor Plans

In a multi-floor facility, a set of tabs at the upper left of the floor plan area controls the display of floors. The leftmost tab displays the default floor, that is, the floor that is normally displayed when there is no alarm activity.

In User mode, alarm activity is displayed on the floor plan at the node location closest to the alarm on the console PCs set up to display alarms from that floor. In a multi-floor facility, the floor where an alarm occurs is immediately displayed no matter which floor is currently displayed. When the alarm is accepted, the display reverts to the default floor.

Important: Floor plans must be an accurately scaled representation of the actual floor (or protected area) in the facility and must be in bitmap (.BMP) format. As well, a floor plan image must be installed for alarm reporting to work properly.

Procedure: Add a Floor Plan

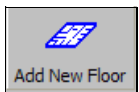
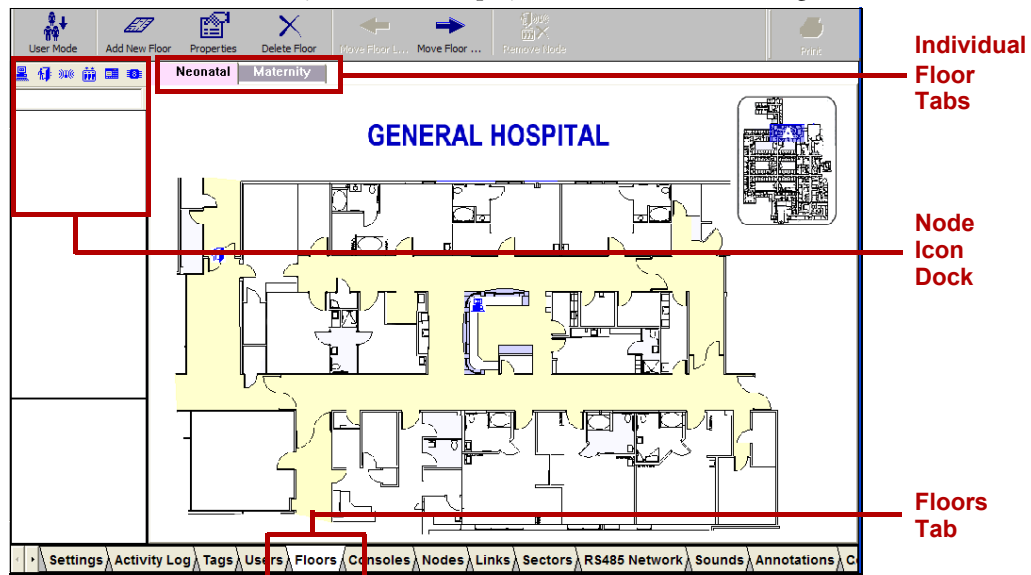
- 1 For every four (4) floor plans, make one photocopy of **Form 9**.
- 2 In the **Setting** column of the form, record the entries you make for each setting. In the column, mark off each setting as you complete it.



- 3 At the RoamAlert server in Administrator mode, select the **Floors** tab.

Note: *The floors displayed in this manual are strictly for demonstration purposes and will not resemble the floors in your facility.*

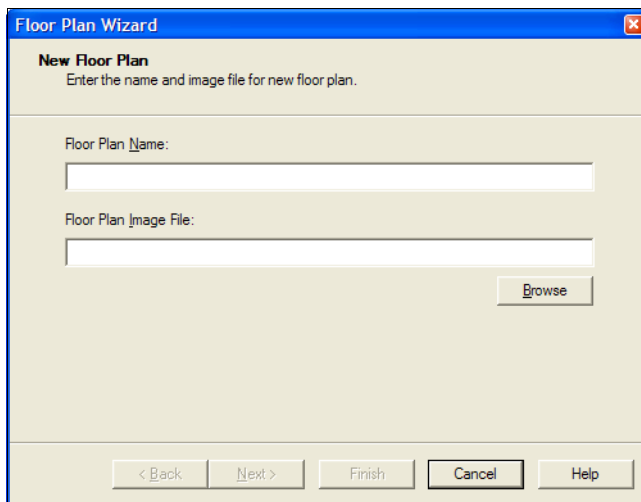
In a multi-floor facility, floors are displayed in tab order, left to right.



- 4 Click **Add New Floor** on the toolbar. The **Floor Plan Wizard** window opens.

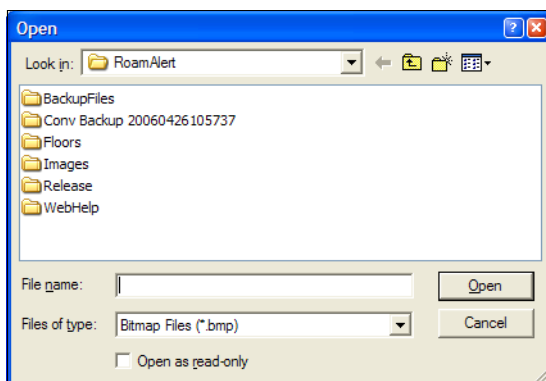


- 5 Click **Next** to continue to the **New Floor Plan** window.



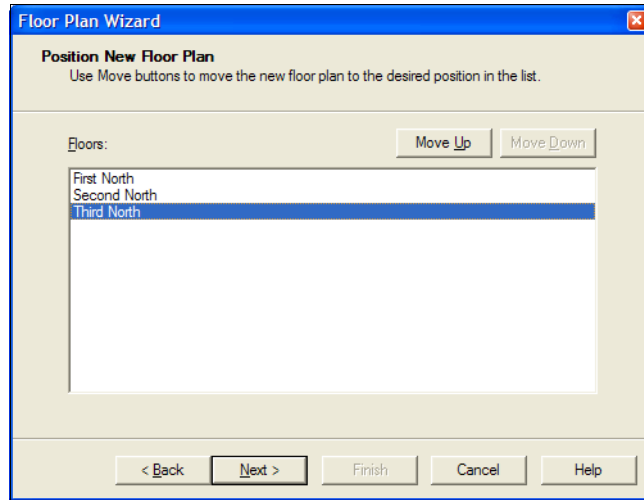
The **Next** button is enabled when both Name and Image file are filled in.

- 6 In the **Floor Plan Name** field, type a short but easily recognizable name to appear on the floor tab.
- 7 Click the **Browse** button. A standard Windows File Open dialog box opens at the RoamAlert Floors folder and displays the available.bmp files. Select the appropriate floor plan file or look in other folders where you may have floor plans stored, select one and click **Open**.



Note: If you have selected a floor plan from outside the RoamAlert Floors folder, RoamAlert automatically copies the plan into the Floors folder.

- Click **Next** to continue to the **Position New Floor Plan** window. The defined floor plan names are listed, with the leftmost in tabbing order at the top and rightmost at the bottom.



- Select the new floor plan and click **Move Up** to bring it toward the top (move the tab left in floor plan view), or **Move Down** to bring it toward the bottom (move the tab right in floor plan view).
- Click **Next** to continue to the **Completing the Floor Plan Wizard** window.



- Review the information you entered for this floor.
If you are not satisfied, click **Back** to make changes, or click **Cancel** to close the wizard without adding the floor.
If you are satisfied, click **Next** to save the floor and start adding another, or click **Finish** to save the floor and close the wizard.
The new floor is added in the defined tab order to the Floors panel.
- Repeat these steps for each floor in the facility.

Place Nodes on Floor Plans

Icons for each node (receivers, console PCs, server PC, controllers, I/O-8 modules) must be placed on the floor plans in the exact location of the node in the facility so that alarms will display correctly at that location.

Note: *Nodes not placed on a floor plan still respond to alarms and other system activity, although the activity will not display on the floor plans.*

The Floors panel includes an Icon Dock at the left which holds the icons for all currently defined nodes in the system.



Above the Icon Dock, a toolbar contains small buttons used to display or hide the icons for a specific node type. This makes icon selection easier when there are many nodes to choose from.

Procedure: Place a Node Icon on a Floor Plan



- 1 At the RoamAlert server in Administrator mode, select the **Floors** tab.
- 2 Select the floor plan on which you will place nodes.



- 3 If necessary, click a button on the Icon Dock toolbar to display the node type you want to place on the floor plan.
If there are more node icons than can be displayed in the dock, you can use the scroll bar, or you can type the ID of the node into the box below the toolbar to bring that node into view.
- 4 Click the node icon and, while holding down the left mouse button, drag the node to the appropriate location on the floor plan, then release the mouse button. The node is added to the floor plan.

Note: *For I/O 8 modules, the module zones are represented by blue (enabled) or purple (disabled) dots. The zone dots can also be dragged and dropped to their correct locations.*

- 5 Repeat Steps 3 and 4 to place all nodes on this floor.
- 6 Update **Form 9 – Floor Settings** when all nodes have been placed on this floor.
- 7 Repeat this procedure for each floor in the facility (as required).

Procedure: Move a Node Icon on a Floor Plan



- 1 At the RoamAlert server in Administrator mode, select the **Floors** tab.
- 2 Select the floor plan which has the node you need to move.
Note: *If you need to move a node icon to another floor in a multi-floor facility, you must first remove the node from the floor plan it is on and then place it on the other floor.*
- 3 On the floor plan, click the node icon and, while holding down the left mouse button, drag the node to its new location, then release the mouse button.

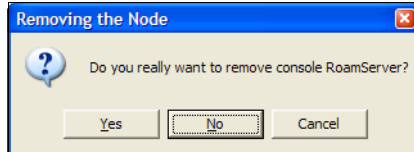
Procedure: Remove a Node Icon from a Floor Plan



- 1 At the RoamAlert server in Administrator mode, select the **Floors** tab.
- 2 Select the floor plan which has the node you need to remove.
- 3 On the floor plan, click the node icon to highlight it. The **Remove Node** button on the Floors panel toolbar is enabled.



- 4 Click **Remove Node** on the Floors panel toolbar.
- 5 Review the information presented in the **Removing the Node** dialog box to make sure that you are removing the correct node.



- 6 Click **No** or **Cancel** to keep the node icon, or click **Yes** to remove it.

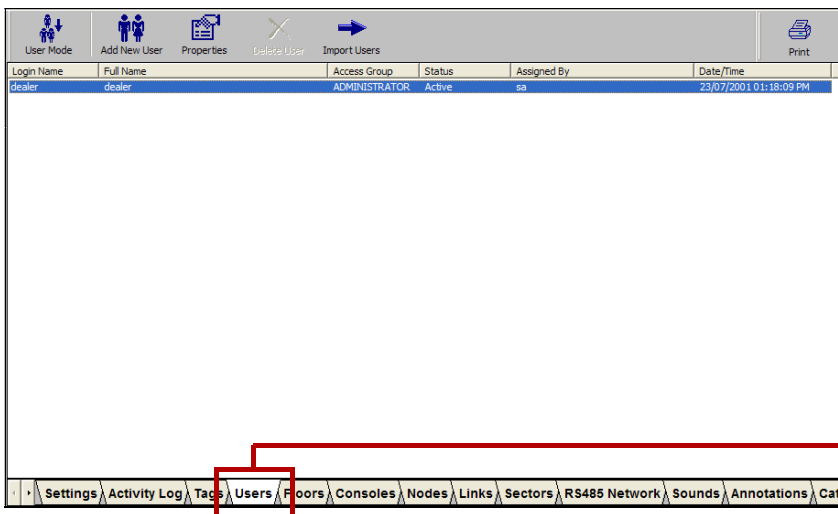
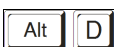
Add Users and Set Access Levels

When a new staff member requires access to RoamAlert, you need to add them to the user list and provide them with a password and an optional PIN code.

If you have many users to add at one time, and you have access to a staff list that is maintained outside of RoamAlert, you can use the Import Users function to retrieve them. See **Appendix B – Importing User Records** for details.

Procedure: Add a New User

- 1 For every ten (10) users, make one photocopy of **Form 10**.
Note: *Alternately, when you have finished adding all users, you could print the user list and include it with the commissioning forms. To print the list, click the **Print** button at the upper right of the Users panel.*
- 2 In the **Setting** column of the form, record the entries you make for each setting. In the ✓ column, mark off each setting as you complete it.
- 3 At the RoamAlert server in Administrator mode, select the **Users** tab.



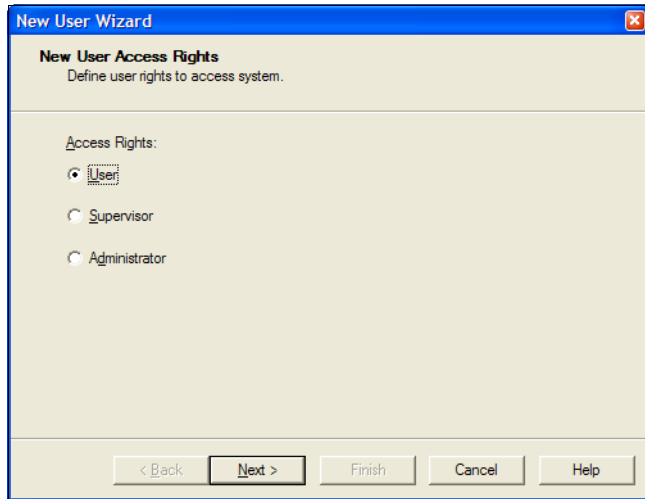
Users
Tab



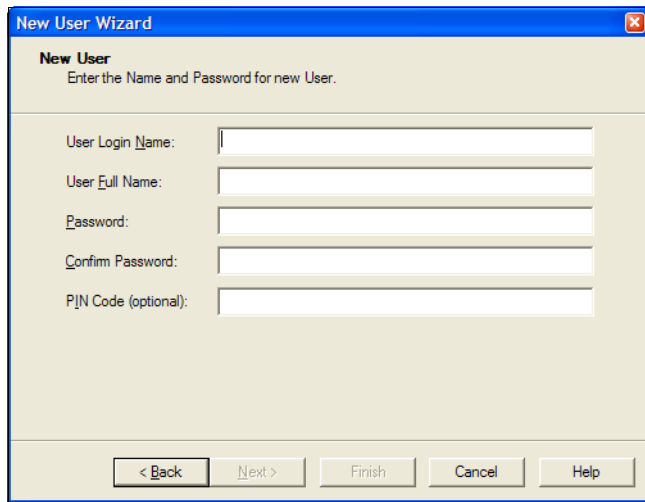
- 4 Click **Add New User** on the toolbar. The **New User Wizard** window opens.



- 5 Click **Next** to continue to the **New User Access Rights** window.



- 6 Click an **Access Rights** button to select the level for this user (see the RoamAlert System Manual for a complete list of tasks by user level), then click **Next** to continue to the **New User** window.

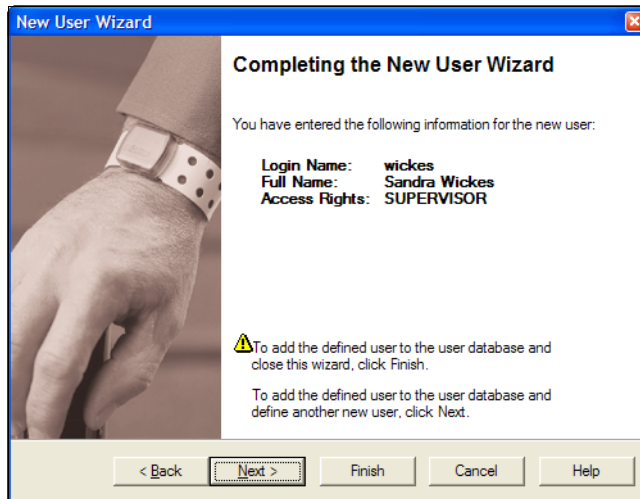


- 7 Fill in the information for this user as follows:

User Login Name	The Login Name must be unique and should be short for quick entry when logging in, (e.g. jsmith for John Smith)
User Full Name	The user's full name, for ease of identification in the list.
Password	A password of at least 6 characters (do not use common constructions such as birthday, child's name, etc.) Case matters: if the password is MistyMint , a login using mistymint will be rejected.
Confirm Password	Enter the password a second time to ensure accuracy (the password appears on screen as a series of *'s)
PIN Code (optional)	If this facility uses this added security feature for access keypad bypass, enter a unique 4-digit PIN (personal identification number) code. If card readers are connected to RoamAlert through a Wiegand interface, the PIN code must be the user's access card ID number.

All fields except PIN Code must be filled in before the **Next** button is enabled.

- 8 Click **Next** to continue to the **Completing the New User Wizard** window.



- 9 Review the information for this new user. If any of the information is not correct:
 - click **Back** to make changes, or
 - click **Cancel** to close the Wizard without adding the user.If you are satisfied with the displayed information:
 - click **Finish** to add this new user and close the New User Wizard, or
 - click **Next** to add this user and begin adding another user.The new user is added to the User List.
- 10 Repeat this procedure for each user you are adding to the system.

Add Tags to Inventory

Tags must be added to the system and their properties set before they can be used, and they should be deleted from the system when their battery life is over.

At the server PC, you have three options for adding tags:

- add the tag manually (any tag),
- read the tag from a Tag Link (wrist, or staff only), or
- read the tag from a controller or receiver (staff tags only).

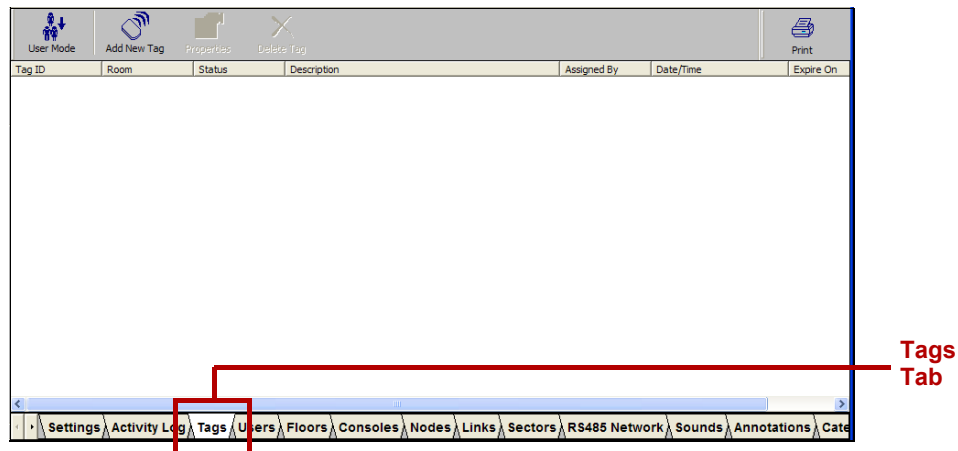
Each of these three methods is described in the procedures below.

Procedure: Prepare to Add Tags

- 1 A form is not provided for tags. When you have finished adding all tags, print the tag list and include it with the commissioning forms. To print the list, click the **Print** button at the upper right of the Tags panel.



- 2 At the RoamAlert server in Administrator mode, select the **Tags** tab.



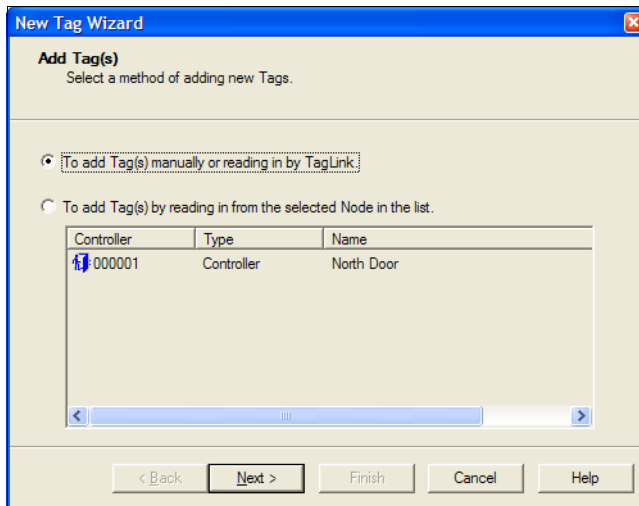
Procedure: Manually Add a Tag (wrist, staff, asset) to Inventory



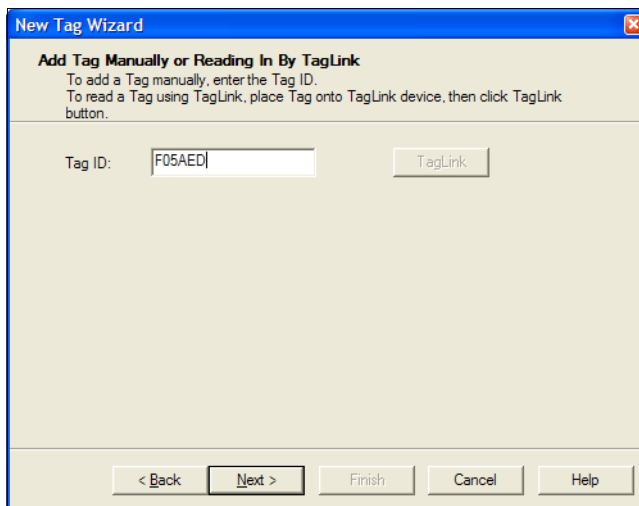
- 1 Click **Add New Tag** on the toolbar. The **New Tag Wizard** window opens.



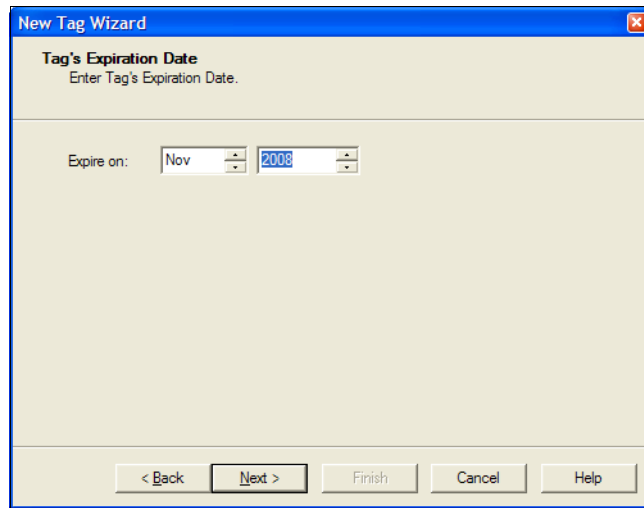
- 2 Click **Next** to continue to the **Add Tag(s)** window.



- 3 Make sure that **To add tag(s) manually or reading in by TagLink** is selected, then click **Next** to continue to the **Add Tag Manually or Reading In By TagLink** window.



- 4 In the **Add Tag Manually or Reading In By TagLink** window, enter the tag ID (found on the foil bag, or the bottom of the wrist tag, then click **Next** to continue to the **Tag's Expiration Date** window.



- 5 Select the month and year of tag expiry using the arrows. The expiry date can be found on the bottom of wrist tags or on the foil bag of wrist and staff tags. If you do not have the foil bag handy, you can use a tag reader to read the expiry date from the tag itself.
- 6 Click **Next** to continue to the **Completing the New Tag Wizard** window.



- 7 Review the information for this tag. If the ID or expiry date are not correct:
 - click **Back** to make changes, or
 - click **Cancel** to close the Wizard without adding the tag.If you are satisfied with the displayed information:
 - click **Finish** to add this new tag and close the New Tag Wizard, or
 - click **Next** to add this tag and begin adding another tag.The new tag is added to the Tag List.
- 8 Repeat this procedures for other tags you are manually adding to the system. Don't forget to print the tag list when all tags have been added.

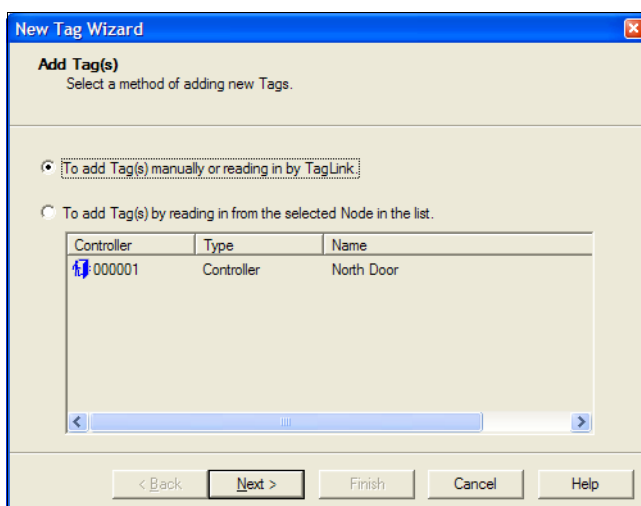
Procedure: Add a Wrist or Staff Tag to Inventory Using the Tag Link



- 1 Click **Add New Tag** on the toolbar. The **New Tag Wizard** window opens.



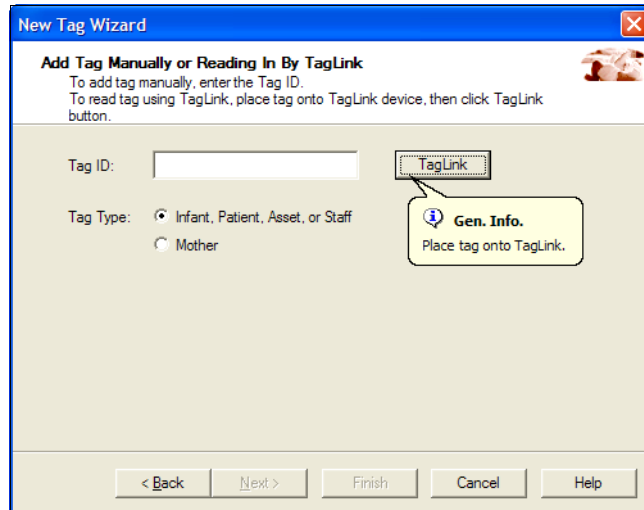
- 2 Click **Next** to continue to the **Add Tag(s)** window.



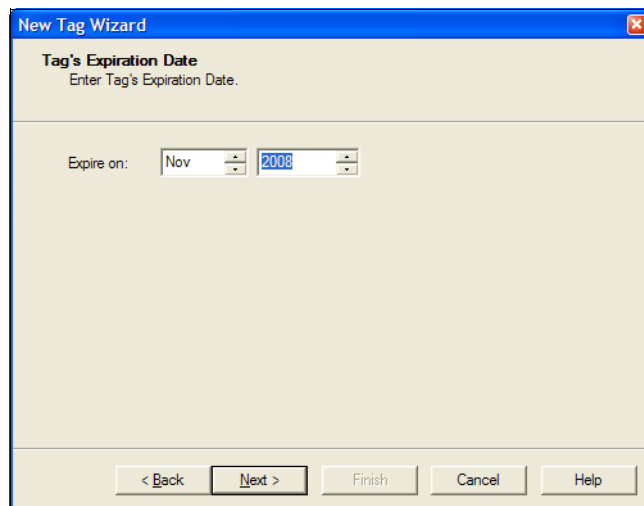
- 3 Make sure that **To add tag(s) manually or reading in by TagLink** is selected, then click **Next** to continue to the **Add Tag Manually or Reading In By TagLink** window.

Note: Make sure the Tag Link is at least two feet away from the computer or monitor to ensure best results.

- 4 Make sure that the Patient, Asset or Staff **Tag Type** is selected.
- 5 Remove the tag from its foil bag, place the tag on the Tag Link, then click the **Tag Link** button.



- 6 The Tag Link reads the tag's ID and expiry date, and RoamAlert opens the **Tag's Expiration Date** window.



- 7 Compare the month and year of expiration in this window with the date on the wrist tag, or the foil bag. If this is not the correct expiry date, select the month and year using the arrows.
- 8 Click **Next** to continue to the **Completing the New Tag Wizard** window.

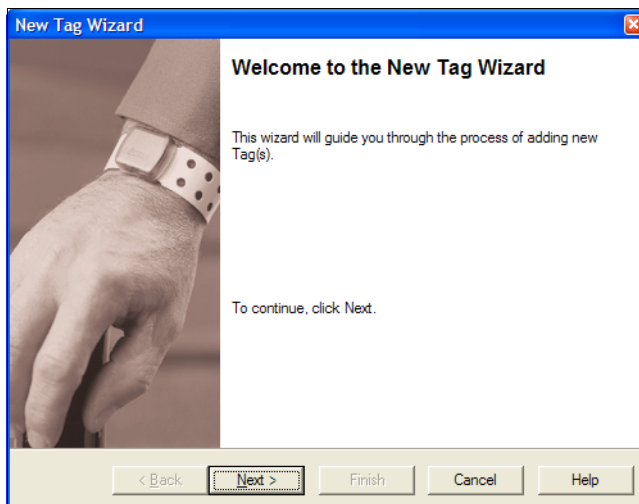


- 9 Review the information for this tag. If the ID or expiry date are not correct:
 - click **Back** to make changes, or
 - click **Cancel** to close the Wizard without adding the tag.
 If you are satisfied with the displayed information:
 - click **Finish** to add this new tag and close the New Tag Wizard, or
 - click **Next** to add this tag and begin adding another tag.
 The new tag is added to the Tag List.
- 10 Repeat this procedures for other tags you are adding to the system using the Tag Link. Don't forget to print the tag list when all tags have been added.

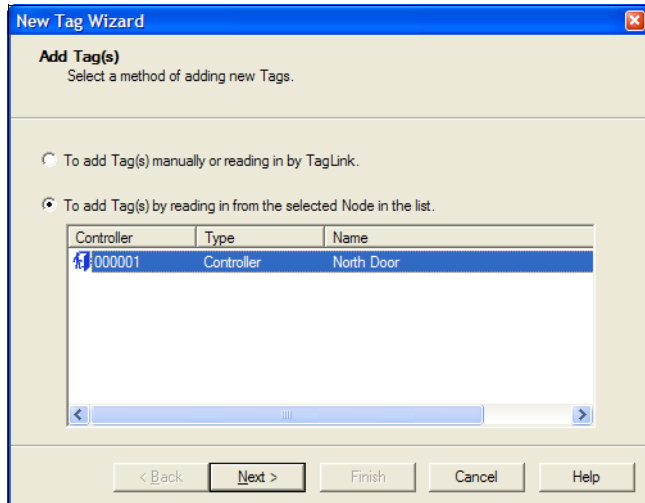
Procedure: Add Multiple Staff Tags at Once to Inventory



- 1 Click **Add New Tag** on the toolbar. The **New Tag Wizard** window opens.

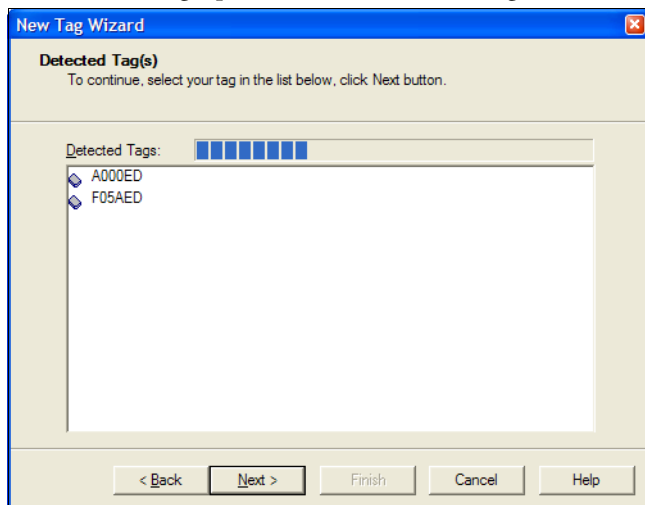


- 2 Click **Next** to continue to the **Add Tag(s)** window.



- 3 Make sure that **To add tag(s) by reading in from the selected Node in the list** is selected, then select the controller or receiver from the list.
- 4 Make sure the tags you want to add are placed within the range of the selected node, then click **Next** to continue to the **Detected Tag(s)** window.

For staff tags, press the button on the tag once.



- 5 When RoamAlert has detected the tags you have placed near the node, which may take a minute or two, click **Next** to continue to the **Completing the New Tag Wizard** window.



6 Review the information for these tags. If the ID or expiry date are not correct:

- click **Back** to make changes, or
- click **Cancel** to close the Wizard without adding the tag.
If you are satisfied with the displayed information:
- click **Finish** to add these new tags and close the New Tag Wizard, or
- click **Next** to add these tags and begin adding other tags.
The new tags are added to the Tag List.

7 Repeat this procedure for other tags you are adding to the system by reading from a node. Don't forget to print the tag list when all tags have been added.

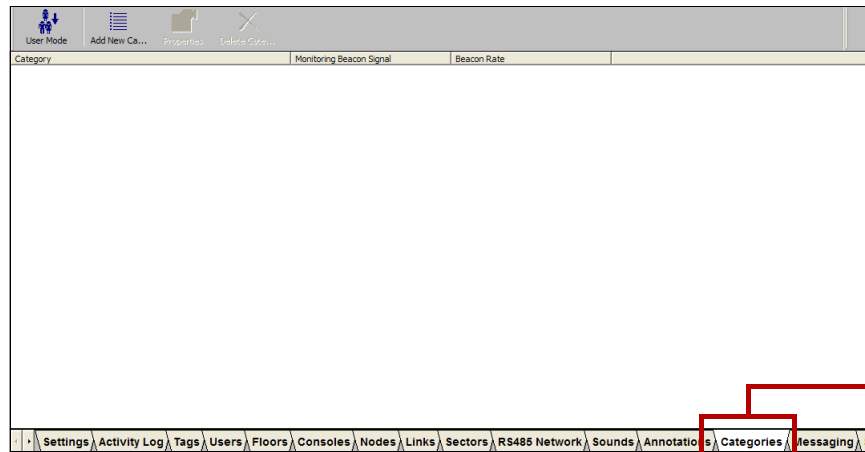
Note: *RoamAlert assumes that the expiry date for all tags detected in this procedure is the same as for the first tag detected. If this is not the case, the expiry date must be edited individually.*

Add and Configure Tag Categories

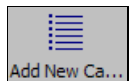
Tag categories are used to group tags into similar classes, such as laptops, IV Pumps, Day Staff, monitors, etc. Tags in the same category will display on the floor plans with the same background color for easy identification. Use these procedures to view and change the categories.

Procedure: Add a New Category

- 1 For every eight (8) categories, make one photocopy of **Form 11**.
- 2 In the **Setting** column of the form, record the entries you make for each setting. In the column, mark off each setting as you complete it.
- 3 At the RoamAlert server in Administrator mode, select the **Categories** tab.



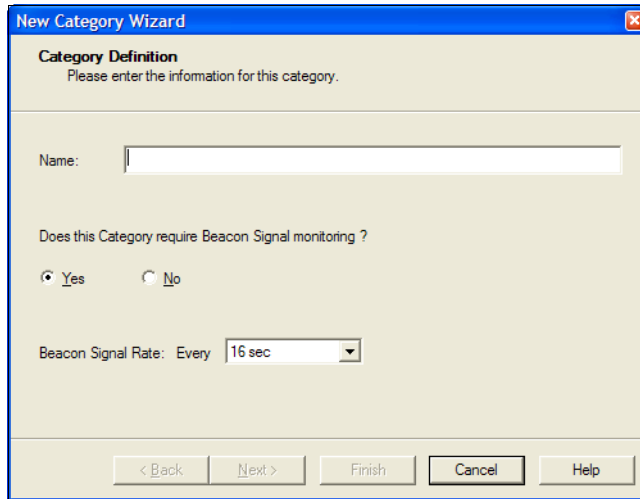
Categories
Tab



- 4 Click **Add New Category** on the toolbar. The **New Category Wizard** window opens.



- 5 Click **Next** to continue to the **Category Definition** window.



6 Fill in the information for this category as follows:

Name	The name must be unique and should be a well-understood definition of the group, e.g. IV Pumps for asset tags or Day Supervisor for staff tags
Beacon Signal Monitoring	<p>Yes: Signals (pulses) from the tags in this category will be monitored. If this category is for staff or asset tags, also select a beacon signal rate from the list. RoamAlert will issue warnings and alarms for missed signals according to the values entered in the Missed Tag Pulse Actions fields on the Settings tab. See Table 4.1, "RoamAlert Configuration Settings" on page 10.</p> <p>No: RoamAlert does not monitor beacon signals for tags in this category. No warnings or alarms are issued if the signal is not detected by a receiver.</p>
Beacon Signal Rate	Use a Tag Reader to set the beacon signal rate of staff or asset tags, then select that rate here. (Cannot be set for wrist tags)
Background Color	Select a color to specify the background displayed for all icons of that category on the floor plans.

Warning

Note: A Beacon Signal is the same as a TLM (tag location message) or tag pulse. Wrist tags with tag pulse emit a signal every 16 seconds. The rate can be configured for staff or asset tags. Beacon (tag pulse) Signal monitoring settings for a category override any settings made to the tag pulse properties of an individual tag.

The **Next** button is enabled when the Name field is filled.

7 Click **Next** to continue to the **Completing the New Category Wizard** window.



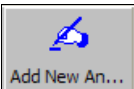
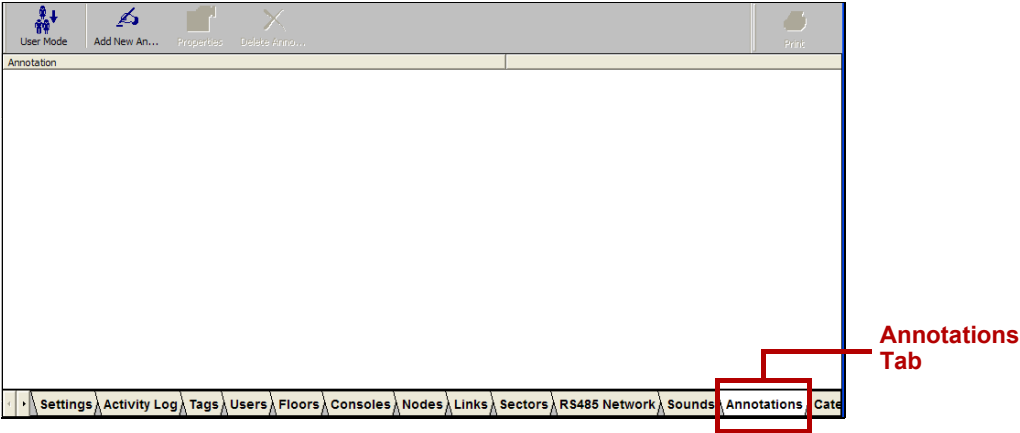
- 8 Review the name for this category.
If you are not satisfied, click **Back** to make changes, or click **Cancel** to close the wizard without adding the category.
If you are satisfied, click **Next** to save the category and start adding another, or click **Finish** to save the category and close the wizard.
The new category is added to the Categories List.
- 9 Repeat this procedure for each category you are adding to the system.

Add Annotations

When a RoamAlert user accepts an alarm, they must supply a reason. This reason, called an **annotation**, may be typed in or selected from a pre-defined list. A pre-defined list makes common reasons available so that typing is minimized and spelling is accurate. Searching the Activity Log for specific annotations is made easier and more accurate as well.

Procedure: Add a New Annotation

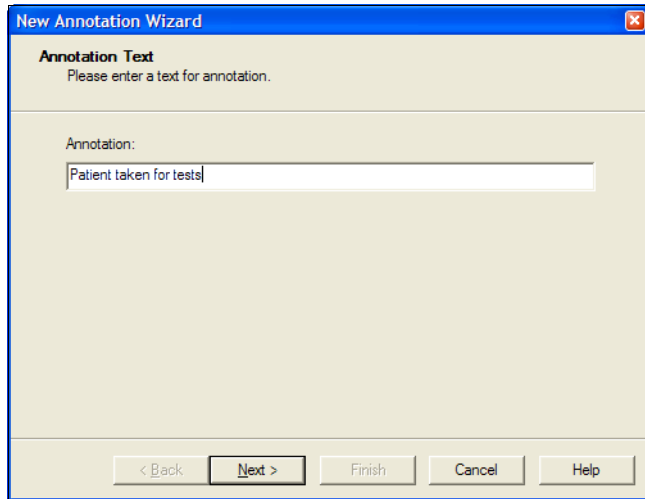
- 1 For every eighteen (18) annotations, make one photocopy of **Form 12**.
- 2 In the **Setting** column of the form, record the entries you make for each setting. In the ✓ column, mark off each setting as you complete it.
- 3 At the RoamAlert server in Administrator mode, select the **Annotations** tab.



- 4 Click **Add New Annotation** on the toolbar. The **New Annotation Wizard** window opens.



- 5 Click **Next** to continue to the **Annotation Text** window.



- 6 Type in the text for this annotation, to a maximum of 120 characters, then click **Next** to continue to the **Completing the New Annotation Wizard** window.



- 7 Review the text for this annotation.
If you are not satisfied, click **Back** to make changes, or click **Cancel** to close the wizard without adding the annotation.
If you are satisfied, click **Next** to save the annotation and start adding another, or click **Finish** to save the annotation and close the wizard.
The annotation is added to the Annotation List.
- 8 Repeat this procedure for each annotation you are adding to the system.

Configure Alarm Sounds

When a tag alarm is received at the server PC, RoamAlert issues the alarm at the server PC or at the console PC designated for that particular alarm. A sound specific to the alarm type and tag is played through the computer speaker.

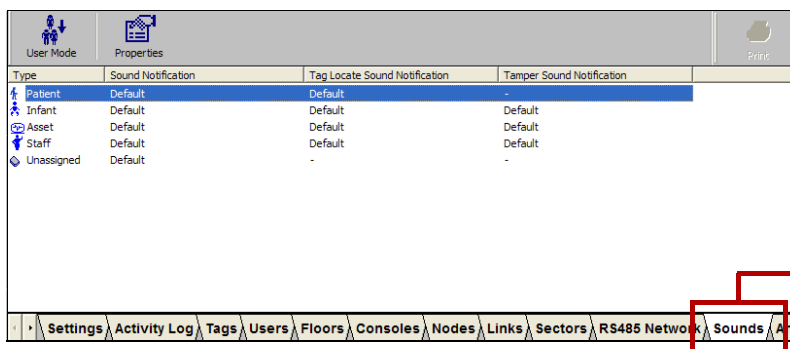
RoamAlert is pre-configured with a default sound for each alarm type (alarm1.wav) and 3 other sounds are supplied (alarm2.wav, alarm3.wav, alarm4.wav) on disk in the RoamAlert installation folder. You can create or sample your own custom alarm sounds using third-party audio software, store them on disk as .wav files and use them in place of the supplied sounds.

You can specify or customize the sound for each type of tag and alarm as follows:

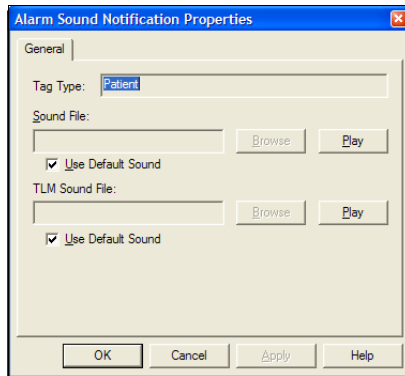
Tag	Exit (TIF)	Locate (TLM)	Tamper (TIC)
Wrist	●	●	
Asset	●	●	●
Staff	●	●	●
Unassigned	●		

Procedure: Change or Customize a Defined Alarm Sound

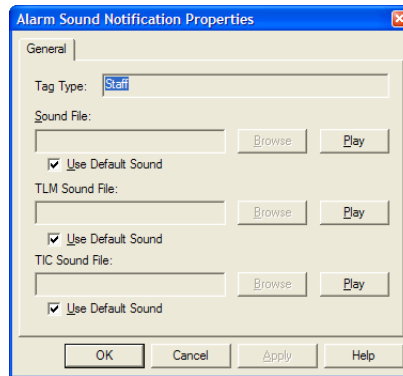
- 1 Make one photocopy of Form 13.
- 2 In the **Setting** column of the form, record the entries you make for each setting. In the ✓ column, mark off each setting as you complete it.
- 3 At the RoamAlert server in Administrator mode, select the **Sounds** tab.



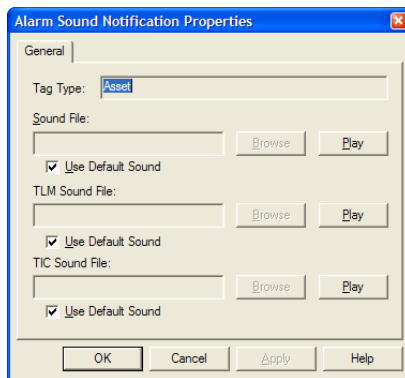
- 4 In the list, double-click the tag type for which you wish to change the sound, or click **Properties** on the toolbar. The **Alarm Sound Notification Properties** sheet opens. The sheet is specific to the tag type.



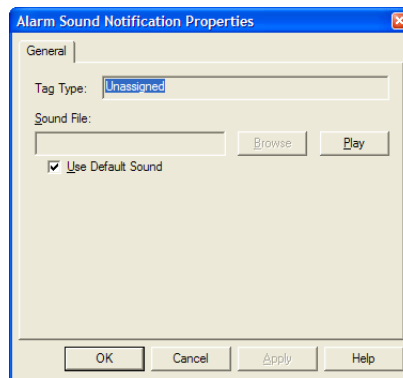
Wrist Tags



Staff Tags

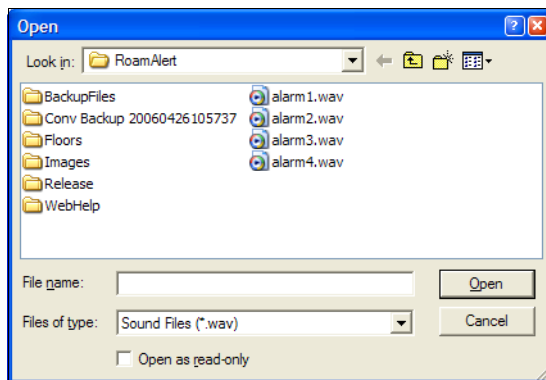


Asset Tags

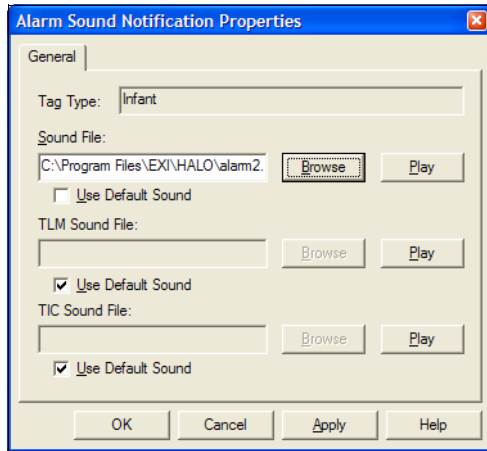


Unassigned Tags

- To change the sound for an alarm type, uncheck the **Use Default Sound** box, then click the **Browse** button. A standard Windows File Open dialog box opens at the RoamAlert installation folder and displays the available .wav files.



- Select one of the displayed .wav files or look in other folders where you may have stored your own custom alarm sounds, select one, then click **Open**. RoamAlert replaces the default sound with the selected one and returns to the properties sheet.



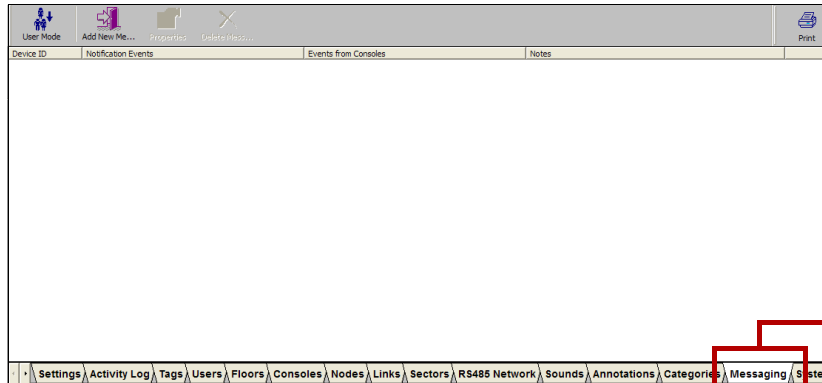
- 7 To test the sound you selected, click **Play**.
- 8 To close the properties sheet without saving your changes, click **Cancel**. To save your changes and close the properties sheet, click **OK**.
- 9 Repeat this procedure for each alarm sound that you want to change or customize.

Add and Configure Messaging Devices

If the facility is implementing alarm communication to messaging devices, such as pagers or wireless handsets, they must be added to the system and configured to receive alarm notifications.

Procedure: Add a New Messaging Device

- 1 For every five (5) devices, make one photocopy of **Form 14**.
- 2 In the **Setting** column of the form, record the entries you make for each setting. In the ✓ column, mark off each setting as you complete it.
- 3 At the RoamAlert server in Administrator mode, select the **Messaging** tab.



- 4 Click **Add New Messaging Device** on the toolbar. The **Messaging Device Wizard** window opens.
- 5 Click **Next** to continue to the **Messaging Device Identification** window.

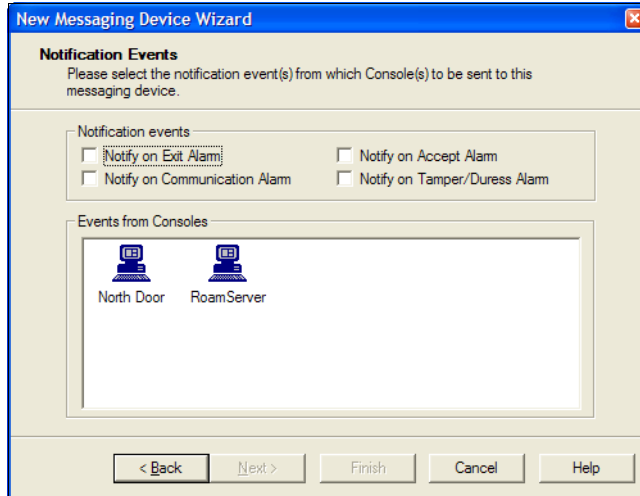
- 6 Fill in the information for this device as follows:

ID The Identification Number of the device, must be unique. Usually found on the device itself.

Notes A brief description of this device, usually the staff member or job position that the device is assigned to, e.g. Night Supervisor or X-ray Technician.

The **Next** button is enabled when the ID field is filled in.

- 7 Click **Next** to continue to the **Notification Events** window. This window displays the four types of event alarms that can be sent to the device, along with an icon for the server PC and each console PC in the system. The **Next** button is not enabled until both an alarm and a console PC are selected.



- 8 Check off the types of alarms to be sent to this device, then select the server PC or console PC from which the alarms will be sent.

Note: If a console PC's **Alarm Filter** has been set to **Can't See** for any node, alarms from that node cannot be sent to the device from the console PC. See "To Add a Console to the RoamAlert System" on page 4-19 for Alarm Filter details.

- 9 Click **Next** to continue to the **Completing the New Messaging Device Wizard** window.



- 10 Review the information you entered for this device.
 - If you are not satisfied, click **Back** to make changes, or click **Cancel** to close the wizard without adding the device.
 - If you are satisfied, click **Next** to save the device and start adding another, or click **Finish** to save the device and close the wizard.

The new device is added to the Messaging Device List.

- 11 Repeat this procedure for each messaging device you are adding to the system.

Add Links

If you are using I/O-8 modules in the installation, links must be defined in order for the output port (or ports) on the module to be activated.

A **Link** is the association between the occurrence of a predefined condition (link trigger) and an operation (link action) that RoamAlert carries out in response.

There are four kinds of triggers that can be defined:

- **Time triggers** cause output ports to be activated at specified times during a day. For example, a time trigger can activate an output port that engages a connected maglock from 8:00 pm to 6:00 am every day.
- **Event triggers** cause I/O-8 output ports to be activated when a system event happens or an I/O-8 input port is activated. For example, an event trigger can activate an output port when an exit alarm (TIF) occurs at a specific controller.
- **Combination triggers** cause output ports to be activated when event trigger conditions are met during a specified time period.

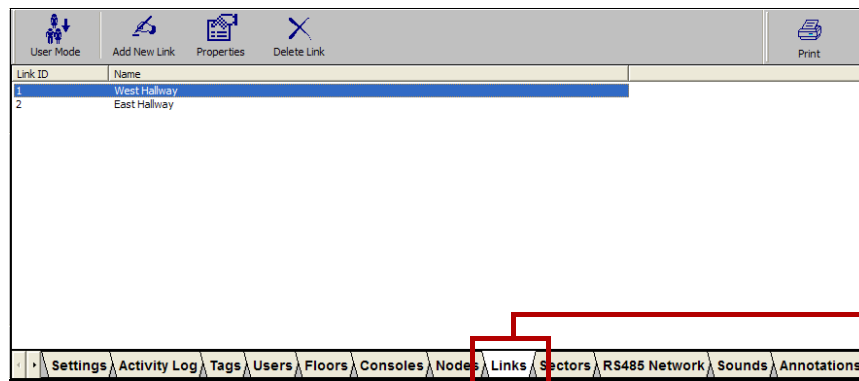
Links require an I/O-8 module with at least one output zone connected and defined in the software. See “Installing an I/O-8 Module” on page 3-38 for physical connections and “Add and Configure Nodes” on page 4-13 for software configuration.

The I/O-8 module can extend RoamAlert functionality for a variety of uses. You can add a door switch to an input zone and configure the zone it to be an input (even supervised). A link can be defined so that whenever the door is opened an output zone activates an external device, such as a CCT camera. This can be a useful scenario if, for example, a door that needs supervision is located in a remote stairwell,

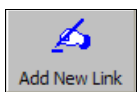
Using this technique, a permitter security network can be configured using I/O-8 modules exclusive of controllers. You could have an entire section of devices being monitored or activated. You could have flow sensors, temperature sensors, flood sensors in a basement, smoke detectors, or any such device connected to the I/O-8 module input zones and linked through output zones to cameras, warning devices etc. The possibilities are virtually unlimited.

Procedure: Add a New Link

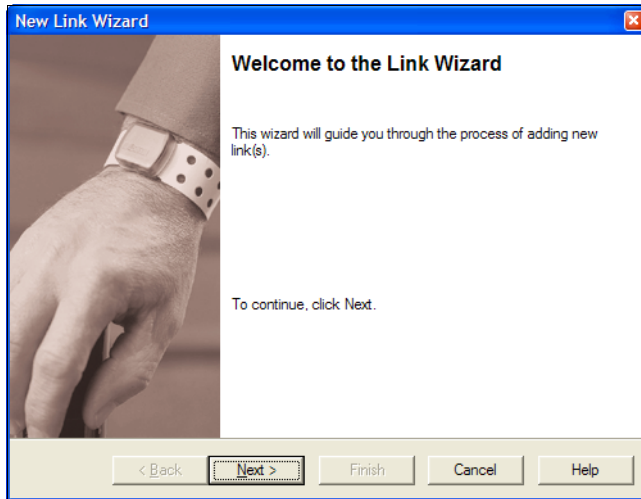
- 1 For each link, make one photocopy of **Form 15**.
- 2 In the **Setting** column of the form, record the entries you make for each setting. In the ✓ column, mark off each setting as you complete it.
- 3 At the RoamAlert server in Administrator mode, select the **Links** tab.



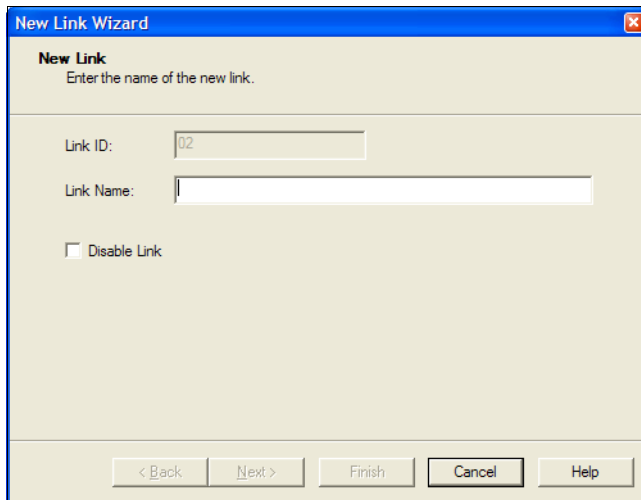
Sectors
Tab



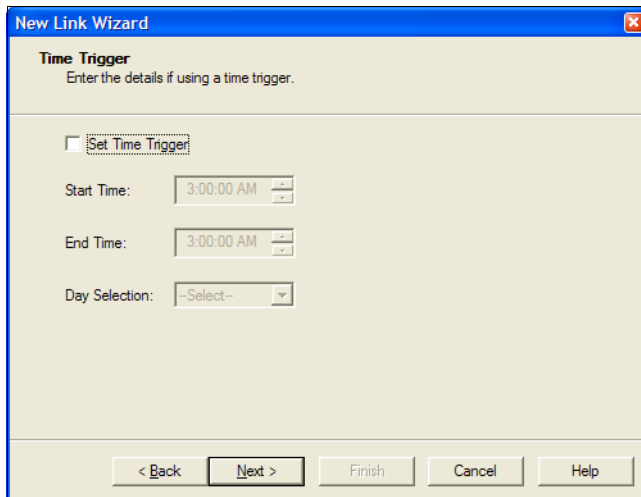
- 4 Click **Add New Link** on the toolbar. The **New Link Wizard** window opens.



- 5 Click **Next** to continue to the **New Link** window.



- 6 Type in a **Link Name** for this link. If you do not want this link to be activated immediately after completing the wizard, check the **Disable Link** box (the link can be activated later in the Property sheet). Click **Next** to continue to the **Time Trigger** window.



- 7 If the link action will **not** be time triggered, click **Next** to continue to the **System Trigger** window. Otherwise, to trigger the link action during a specific time period on one or more days of the week:

7.1 Check the **Set Time Trigger** box.

7.2 Select a **Start Time** and an **End Time** for the trigger. Click the hour, minutes, or seconds and use the arrows to increase or decrease the value. The End Time must be later than the Start Time.

A screenshot of a form titled "Set Time Trigger". It features a checked checkbox labeled "Set Time Trigger". Below the checkbox are two time selection fields: "Start Time" set to "3:00:00 AM" and "End Time" set to "6:00:00 AM". Each field has small up/down arrows for adjustment.

7.3 Select a day or day range from the **Day Selection** list. You can set the trigger to occur any day of the week (Mon-Sun), just weekdays (Mon-Fri), just weekends (Sat-Sun), or only on a specific day of the week.

A screenshot of the "New Link Wizard" window, specifically the "Time Trigger" section. The title bar says "New Link Wizard". Below the title bar, it says "Time Trigger" and "Enter the details if using a time trigger." There is a checked checkbox "Set Time Trigger". Below it are "Start Time" (3:00:00 AM) and "End Time" (3:00:00 AM) fields. A "Day Selection" dropdown menu is set to "--Select--". At the bottom are buttons for "< Back", "Next >", "Finish", "Cancel", and "Help".

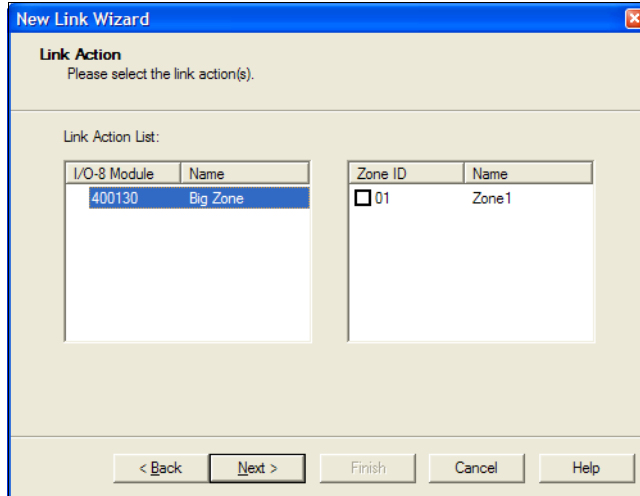
7.4 When you are satisfied with the time trigger setting, click **Next** to continue to the **System Trigger** window.

- 8 In the **System Trigger** window, you can set up one or more system inputs that trigger the link action.

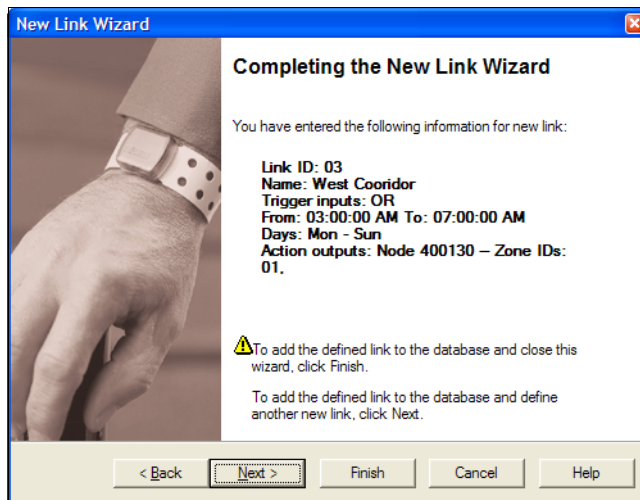
A screenshot of the "New Link Wizard" window, specifically the "System Trigger" section. The title bar says "New Link Wizard". Below the title bar, it says "System Trigger" and "Enter the details if using a system trigger." There is a "Logic Type" section with radio buttons for "AND" and "OR", with "OR" selected. Below this are two tables. The first table has columns "Controller" and "Name" and lists two entries: "104636 North Door" and "400130 West Corridor". The second table has columns "Input" and "Name" and lists four entries: "Bypass On" (checked), "Door Open", "Exit Alarm", and "Field Occupied". At the bottom are buttons for "< Back", "Next >", "Finish", "Cancel", and "Help".

If the link action is only time triggered and not system event triggered, click **Next** to continue to the **Link Action** window. Otherwise, to set a system event trigger:

- 8.1 Select a **Controller** (or I/O-8 module) and then select an **Input** type.
 - 8.2 If two or more inputs are used to trigger the link action, select the **Logic Type**. The **AND** type triggers the link action when all the defined inputs occur, the **OR** type when any of the inputs occurs.
 - 8.3 Click **Next** to continue to the **Link Action** window.
- 9 In the Link Action window, you specify the I/O-8 module output zone that will be activated when the trigger conditions are met.



- 10 Select the **I/O-8 Module** and then check the output zones to be activated.
- 11 Click **Next** to continue to the **Completing the New Link Wizard** window.
- 12 In the Completing the New Link Wizard window, review the information you entered for this link.



- click **Back** to make changes, or
 - click **Cancel** to close the Wizard without adding the link.
- If you are satisfied with the displayed information:
- click **Next** to add this link and begin adding another link, or

- click **Finish** to add this new link and close the New Link Wizard.
The new link is added to the Link List.

13 Repeat this procedure for each new link you are adding to the system.

SYSTEM COMMISSIONING

This chapter describes the tasks required to commission the system for use.

When all devices and software have been installed and configured, a final system check must be performed before the system is commissioned. System commissioning tasks include:

- performing the final system check,
- documenting the software and hardware as installed, and
- delivering the system and documentation to the client.

Performing the Final System Check

This is essentially a functionality test, where you make sure that all the components and features that have been installed and configured are verified and documented.

Door Controllers

Check the operation of each door controller:

- walk into the detection field at a door with an admitted tag, which should lock the door (if so configured) and start an audible warning (TIF) at the local keypad.
- complete a bypass at each keypad to ensure correct operation.

Elevator Controllers

Check the operation of each elevator controller:

- walk into the detection field at an elevator door with an admitted tag, which should lock the door open and start an audible warning (TIF) at the local keypad.
- complete a bypass at each keypad to ensure correct operation.

Receivers

Check the operation of each receiver:

- with a test tag, move about the entire protected area and ensure that the tag is detected at all locations in all possible orientations.
- if the site is using TLM (tag location monitoring), several admitted tags should be deployed throughout the protected area to collect tag pulse statistics. These statistics can then be analyzed to determine if coverage is adequate. Tag pulse statistics can be viewed on the Tag Pulse Supervision tab of a tag's property sheet. Refer to the RoamAlert System Manual, Chapter 6, Tag Management for details.
- TLM coverage can only be confirmed after tags are deployed on residents and statistics collected for a reasonable period (at least two weeks). You should then review these statistics to ensure that coverage is in place to adequately monitor TLM.

Documenting the Installed Software and Hardware

You should develop a System Commissioning Report in a three-ring tabbed binder that contains all completed forms, printouts of floor plans with devices located, and any other information that may be useful to the client.

Software

Follow the procedures in **Chapter 4 – Software Configuration** and add all completed forms to the System Commissioning binder that you will turn over to the client at system delivery.

Hardware

Door Controllers

For each door controller, print and complete **Form 16**.

Elevator Controllers

For each elevator controller, print and complete **Form 17**.

Receivers

For each receiver, print and complete **Form 18**.

Add these completed forms to the System Commissioning binder.

Delivering the System to the Client

The administrator of the system will have to be shown that the system is functioning properly so that it can be signed off. We strongly recommend that you involve at least this person in the commissioning phase so that they can become familiar with the system, while at the same time they are provided training in a natural way.

Once the system is shown to be functioning according to specifications, a signature can be obtained to mark the official transfer of operational, and possibly maintenance, responsibility.

The client should have been made aware that the original quotation represented an estimate of the equipment required to provide adequate protection, since RF installation is not an exact science. Environmental factors that cannot be foreseen have a strong impact on RF coverage.

Agreement with the client on deliverables should be part of initial contract negotiations. Along with a tested system, deliverables might include:

- as-built drawings,
- equipment lists, and
- administrator and user training.



COMMISSIONING FORMS

This appendix contains the following commissioning forms:

Page	Form Name	Usage
Software Forms		
A-2	Software Configuration Checklist	Initial and enter task completion dates
A-3	RoamAlert Configuration Settings	1 copy
A-5	Door Controller Settings	1 copy for every four (4) door controllers
A-6	Elevator Controller Settings	1 copy for every six (6) elevator controllers
A-7	Receiver Settings	1 copy for every six (6) receivers
A-8	I/O-8 Module Settings	1 copy for each I/O-8 module
A-9	Remote Display Unit (RDU) Settings	1 copy for each RDU + 1 copy of each Alarm Filter page for every 20 controllers, receivers, or I/O-8 modules
A-10	RoamAlert Server/Console PC Settings	1 copy for each server or console + 1 copy of each Alarm Filter page for every 20 controllers, receivers, or I/O-8 modules
A-14	Floor Settings	1 copy for every four (4) floor plans
A-15	User Settings	1 copy for every ten(10) users
A-16	Category Settings	1 copy for every eight (8) categories
A-17	Annotation Settings	1 copy for every eighteen (18) annotations
A-18	Alarm Sound Settings	1 copy
A-19	Messaging Device Settings	1 copy for every five (5) devices
A-20	Link Settings	1 copy for each link
Hardware Forms		
A-21	Door Controller Hardware Settings	1 copy for each door controller
A-22	Elevator Controller Hardware Settings	1 copy for each elevator controller
A-23	Receiver Hardware Settings	1 copy for each receiver

Form 1 Software Configuration Checklist

Task	Technician Name/Initials	Date Completed (YYYY/MM/DD)
RoamAlert Global Settings		____/____/____
RS485 Network		____/____/____
Door Controllers		____/____/____
Elevator Controllers		____/____/____
Receivers		____/____/____
I/O-8 Modules		____/____/____
Remote Display Units		____/____/____
Network Managers		____/____/____
Server/Consoles		____/____/____
Floors and Node Placement		____/____/____
Users		____/____/____
Tags		____/____/____
Tag Categories		____/____/____
Annotations		____/____/____
Alarm Sounds		____/____/____
Messaging Devices		____/____/____
Links		____/____/____
Notes:		

Form 2 RoamAlert Configuration Settings

Item	Setting	✓
General		
Filter Door Events	Default = Enabled Setting = <input type="checkbox"/> (Enable is recommended)	<input type="checkbox"/>
Show Noise Status	Default = Disabled Setting = <input type="checkbox"/>	<input type="checkbox"/>
Nurse Saver Mode	Default = Disabled Setting = <input type="checkbox"/>	<input type="checkbox"/>
Use Screen Saver	Default = Disabled Setting = <input type="checkbox"/>	<input type="checkbox"/>
Enable Mute Button	Default = Enabled Setting = <input type="checkbox"/>	<input type="checkbox"/>
Alarm on Unassigned TIF	Default = Disabled Setting = <input type="checkbox"/>	<input type="checkbox"/>
On Screen Keyboard	Default = Disabled Setting = <input type="checkbox"/>	<input type="checkbox"/>
Use Small Icon Size	Default = Disabled Setting = <input type="checkbox"/>	<input type="checkbox"/>
Warn on Tags Not In Inventory	Default = Disabled Setting = <input type="checkbox"/>	<input type="checkbox"/>
Activity Log		
Keep Last nn Days	Default = 31 days Select a new value if necessary Days in log: _____	<input type="checkbox"/>
Backup		
Backup Folder	Default = C:\Program Files\EXI\RoamAlert\BackupFiles Alternate folder selected: _____ _____	<input type="checkbox"/>
RDU Audible Alert Profile		
Profile # 1: Day <input type="checkbox"/> Night: <input type="checkbox"/>	Start ___:___:___ AM / PM End ___:___:___ AM / PM	<input type="checkbox"/>
Profile # 2: Day <input type="checkbox"/> Night: <input type="checkbox"/>	Start ___:___:___ AM / PM End ___:___:___ AM / PM	<input type="checkbox"/>
Profile # 3: Day <input type="checkbox"/> Night: <input type="checkbox"/>	Start ___:___:___ AM / PM End ___:___:___ AM / PM	<input type="checkbox"/>
Profile # 4: Day <input type="checkbox"/> Night: <input type="checkbox"/>	Start ___:___:___ AM / PM End ___:___:___ AM / PM	<input type="checkbox"/>
Profile # 5: Day <input type="checkbox"/> Night: <input type="checkbox"/>	Start ___:___:___ AM / PM End ___:___:___ AM / PM	<input type="checkbox"/>
Profile # 6: Day <input type="checkbox"/> Night: <input type="checkbox"/>	Start ___:___:___ AM / PM End ___:___:___ AM / PM	<input type="checkbox"/>
Profile # 7: Day <input type="checkbox"/> Night: <input type="checkbox"/>	Start ___:___:___ AM / PM End ___:___:___ AM / PM	<input type="checkbox"/>
Profile # 8: Day <input type="checkbox"/> Night: <input type="checkbox"/>	Start ___:___:___ AM / PM End ___:___:___ AM / PM	<input type="checkbox"/>
Missed Tag Pulse Actions		
nn missed TLMs to Warning	Default = 2 Enter new value if changed: _____	<input type="checkbox"/>
nn missed TLMs to Alarm	Default = 4 Enter new value if changed: _____	<input type="checkbox"/>
Suppress Visual and Audio Annunciation	Default = Disabled Setting = <input type="checkbox"/>	<input type="checkbox"/>

Form 2 RoamAlert Configuration Settings (continued)

Item	Setting	✓
User Authentication (Enable recommended)		
Shutdown System	Default = Disabled Setting = <input type="checkbox"/>	<input type="checkbox"/>
Accept Alarm	Default = Disabled Setting = <input type="checkbox"/>	<input type="checkbox"/>
Perform User Functions	Default = Disabled Setting = <input type="checkbox"/>	<input type="checkbox"/>
Enter Supervisor Mode	Default = Disabled Setting = <input type="checkbox"/>	<input type="checkbox"/>
Enter Administrator Mode	Default = Disabled Setting = <input type="checkbox"/>	<input type="checkbox"/>
Messaging Port Settings		
Serial Port	Default = None Port selected: _____	<input type="checkbox"/>
Baud Rate	Default = 9600 Baud rate selected: _____	<input type="checkbox"/>
System Background Color		
Change Current Selection	Default = Red: 192, Green: 192, Blue: 192 New selected background color: Red: ____ Green: ____ Blue: ____	<input type="checkbox"/>

Form 3 Door Controller Settings

Item	Setting	✓
------	---------	---

Door Controller # ____

New Node		
Serial Number	Number = _____	<input type="checkbox"/>
Node Name	Name = _____	<input type="checkbox"/>
Door Controller Operation Modes		
Door Ajar Alarm	<input type="checkbox"/> Door Ajar Alarm after ____ seconds	<input type="checkbox"/>
Suppress Loiter	<input type="checkbox"/> Suppress Loiter	<input type="checkbox"/>

Door Controller # ____

New Node		
Serial Number	Number = _____	<input type="checkbox"/>
Node Name	Name = _____	<input type="checkbox"/>
Door Controller Operation Modes		
Door Ajar Alarm	<input type="checkbox"/> Door Ajar Alarm after ____ seconds	<input type="checkbox"/>
Suppress Loiter	<input type="checkbox"/> Suppress Loiter	<input type="checkbox"/>

Door Controller # ____

New Node		
Serial Number	Number = _____	<input type="checkbox"/>
Node Name	Name = _____	<input type="checkbox"/>
Door Controller Operation Modes		
Door Ajar Alarm	<input type="checkbox"/> Door Ajar Alarm after ____ seconds	<input type="checkbox"/>
Suppress Loiter	<input type="checkbox"/> Suppress Loiter	<input type="checkbox"/>

Door Controller # ____

New Node		
Serial Number	Number = _____	<input type="checkbox"/>
Node Name	Name = _____	<input type="checkbox"/>
Door Controller Operation Modes		
Door Ajar Alarm	<input type="checkbox"/> Door Ajar Alarm after ____ seconds	<input type="checkbox"/>
Suppress Loiter	<input type="checkbox"/> Suppress Loiter	<input type="checkbox"/>

Form 4 Elevator Controller Settings

Item	Setting	✓
------	---------	---

Elevator Controller # ____

New Node		
Serial Number	Number = _____	<input type="checkbox"/>
Node Name	Name = _____	<input type="checkbox"/>

Elevator Controller # ____

New Node		
Serial Number	Number = _____	<input type="checkbox"/>
Node Name	Name = _____	<input type="checkbox"/>

Elevator Controller # ____

New Node		
Serial Number	Number = _____	<input type="checkbox"/>
Node Name	Name = _____	<input type="checkbox"/>

Elevator Controller # ____

New Node		
Serial Number	Number = _____	<input type="checkbox"/>
Node Name	Name = _____	<input type="checkbox"/>

Elevator Controller # ____

New Node		
Serial Number	Number = _____	<input type="checkbox"/>
Node Name	Name = _____	<input type="checkbox"/>

Elevator Controller # ____

New Node		
Serial Number	Number = _____	<input type="checkbox"/>
Node Name	Name = _____	<input type="checkbox"/>

Form 5 Receiver Settings

Item	Setting	✓
------	---------	---

Receiver # _____

New Node		
Serial Number	Number = _____	<input type="checkbox"/>
Node Name	Name = _____	<input type="checkbox"/>

Receiver # _____

New Node		
Serial Number	Number = _____	<input type="checkbox"/>
Node Name	Name = _____	<input type="checkbox"/>

Receiver # _____

New Node		
Serial Number	Number = _____	<input type="checkbox"/>
Node Name	Name = _____	<input type="checkbox"/>

Receiver # _____

New Node		
Serial Number	Number = _____	<input type="checkbox"/>
Node Name	Name = _____	<input type="checkbox"/>

Receiver # _____

New Node		
Serial Number	Number = _____	<input type="checkbox"/>
Node Name	Name = _____	<input type="checkbox"/>

Receiver # _____

New Node		
Serial Number	Number = _____	<input type="checkbox"/>
Node Name	Name = _____	<input type="checkbox"/>

Form 6 I/O-8 Module Settings

Item	Setting	✓				
New Node						
Serial Number	_____	<input type="checkbox"/>				
Node Name	_____	<input type="checkbox"/>				
Configure I/O-8 Zone Settings						
Zone 1	Name = _____ Enabled <input type="checkbox"/> Assigned <input type="checkbox"/>	<input type="checkbox"/>				
	<table border="0" style="width: 100%;"> <tr> <td style="width: 50%;">Output <input type="checkbox"/></td> <td style="width: 50%;">Input <input type="checkbox"/></td> </tr> <tr> <td>Non-Active <input type="checkbox"/> Active <input type="checkbox"/></td> <td>Type: Latch <input type="checkbox"/> Non-Latch <input type="checkbox"/></td> </tr> <tr> <td></td> <td>State: NC <input type="checkbox"/> NO <input type="checkbox"/> Supervised: <input type="checkbox"/></td> </tr> </table>		Output <input type="checkbox"/>	Input <input type="checkbox"/>	Non-Active <input type="checkbox"/> Active <input type="checkbox"/>	Type: Latch <input type="checkbox"/> Non-Latch <input type="checkbox"/>
Output <input type="checkbox"/>	Input <input type="checkbox"/>					
Non-Active <input type="checkbox"/> Active <input type="checkbox"/>	Type: Latch <input type="checkbox"/> Non-Latch <input type="checkbox"/>					
	State: NC <input type="checkbox"/> NO <input type="checkbox"/> Supervised: <input type="checkbox"/>					
Zone 2	Name = _____ Enabled <input type="checkbox"/> Assigned <input type="checkbox"/>	<input type="checkbox"/>				
	<table border="0" style="width: 100%;"> <tr> <td style="width: 50%;">Output <input type="checkbox"/></td> <td style="width: 50%;">Input <input type="checkbox"/></td> </tr> <tr> <td>Non-Active <input type="checkbox"/> Active <input type="checkbox"/></td> <td>Type: Latch <input type="checkbox"/> Non-Latch <input type="checkbox"/></td> </tr> <tr> <td></td> <td>State: NC <input type="checkbox"/> NO <input type="checkbox"/> Supervised: <input type="checkbox"/></td> </tr> </table>		Output <input type="checkbox"/>	Input <input type="checkbox"/>	Non-Active <input type="checkbox"/> Active <input type="checkbox"/>	Type: Latch <input type="checkbox"/> Non-Latch <input type="checkbox"/>
Output <input type="checkbox"/>	Input <input type="checkbox"/>					
Non-Active <input type="checkbox"/> Active <input type="checkbox"/>	Type: Latch <input type="checkbox"/> Non-Latch <input type="checkbox"/>					
	State: NC <input type="checkbox"/> NO <input type="checkbox"/> Supervised: <input type="checkbox"/>					
Zone 3	Name = _____ Enabled <input type="checkbox"/> Assigned <input type="checkbox"/>	<input type="checkbox"/>				
	<table border="0" style="width: 100%;"> <tr> <td style="width: 50%;">Output <input type="checkbox"/></td> <td style="width: 50%;">Input <input type="checkbox"/></td> </tr> <tr> <td>Non-Active <input type="checkbox"/> Active <input type="checkbox"/></td> <td>Type: Latch <input type="checkbox"/> Non-Latch <input type="checkbox"/></td> </tr> <tr> <td></td> <td>State: NC <input type="checkbox"/> NO <input type="checkbox"/> Supervised: <input type="checkbox"/></td> </tr> </table>		Output <input type="checkbox"/>	Input <input type="checkbox"/>	Non-Active <input type="checkbox"/> Active <input type="checkbox"/>	Type: Latch <input type="checkbox"/> Non-Latch <input type="checkbox"/>
Output <input type="checkbox"/>	Input <input type="checkbox"/>					
Non-Active <input type="checkbox"/> Active <input type="checkbox"/>	Type: Latch <input type="checkbox"/> Non-Latch <input type="checkbox"/>					
	State: NC <input type="checkbox"/> NO <input type="checkbox"/> Supervised: <input type="checkbox"/>					
Zone 4	Name = _____ Enabled <input type="checkbox"/> Assigned <input type="checkbox"/>	<input type="checkbox"/>				
	<table border="0" style="width: 100%;"> <tr> <td style="width: 50%;">Output <input type="checkbox"/></td> <td style="width: 50%;">Input <input type="checkbox"/></td> </tr> <tr> <td>Non-Active <input type="checkbox"/> Active <input type="checkbox"/></td> <td>Type: Latch <input type="checkbox"/> Non-Latch <input type="checkbox"/></td> </tr> <tr> <td></td> <td>State: NC <input type="checkbox"/> NO <input type="checkbox"/> Supervised: <input type="checkbox"/></td> </tr> </table>		Output <input type="checkbox"/>	Input <input type="checkbox"/>	Non-Active <input type="checkbox"/> Active <input type="checkbox"/>	Type: Latch <input type="checkbox"/> Non-Latch <input type="checkbox"/>
Output <input type="checkbox"/>	Input <input type="checkbox"/>					
Non-Active <input type="checkbox"/> Active <input type="checkbox"/>	Type: Latch <input type="checkbox"/> Non-Latch <input type="checkbox"/>					
	State: NC <input type="checkbox"/> NO <input type="checkbox"/> Supervised: <input type="checkbox"/>					
Zone 5	Name = _____ Enabled <input type="checkbox"/> Assigned <input type="checkbox"/>	<input type="checkbox"/>				
	<table border="0" style="width: 100%;"> <tr> <td style="width: 50%;">Output <input type="checkbox"/></td> <td style="width: 50%;">Input <input type="checkbox"/></td> </tr> <tr> <td>Non-Active <input type="checkbox"/> Active <input type="checkbox"/></td> <td>Type: Latch <input type="checkbox"/> Non-Latch <input type="checkbox"/></td> </tr> <tr> <td></td> <td>State: NC <input type="checkbox"/> NO <input type="checkbox"/> Supervised: <input type="checkbox"/></td> </tr> </table>		Output <input type="checkbox"/>	Input <input type="checkbox"/>	Non-Active <input type="checkbox"/> Active <input type="checkbox"/>	Type: Latch <input type="checkbox"/> Non-Latch <input type="checkbox"/>
Output <input type="checkbox"/>	Input <input type="checkbox"/>					
Non-Active <input type="checkbox"/> Active <input type="checkbox"/>	Type: Latch <input type="checkbox"/> Non-Latch <input type="checkbox"/>					
	State: NC <input type="checkbox"/> NO <input type="checkbox"/> Supervised: <input type="checkbox"/>					
Zone 6	Name = _____ Enabled <input type="checkbox"/> Assigned <input type="checkbox"/>	<input type="checkbox"/>				
	<table border="0" style="width: 100%;"> <tr> <td style="width: 50%;">Output <input type="checkbox"/></td> <td style="width: 50%;">Input <input type="checkbox"/></td> </tr> <tr> <td>Non-Active <input type="checkbox"/> Active <input type="checkbox"/></td> <td>Type: Latch <input type="checkbox"/> Non-Latch <input type="checkbox"/></td> </tr> <tr> <td></td> <td>State: NC <input type="checkbox"/> NO <input type="checkbox"/> Supervised: <input type="checkbox"/></td> </tr> </table>		Output <input type="checkbox"/>	Input <input type="checkbox"/>	Non-Active <input type="checkbox"/> Active <input type="checkbox"/>	Type: Latch <input type="checkbox"/> Non-Latch <input type="checkbox"/>
Output <input type="checkbox"/>	Input <input type="checkbox"/>					
Non-Active <input type="checkbox"/> Active <input type="checkbox"/>	Type: Latch <input type="checkbox"/> Non-Latch <input type="checkbox"/>					
	State: NC <input type="checkbox"/> NO <input type="checkbox"/> Supervised: <input type="checkbox"/>					
Zone 7	Name = _____ Enabled <input type="checkbox"/> Assigned <input type="checkbox"/>	<input type="checkbox"/>				
	<table border="0" style="width: 100%;"> <tr> <td style="width: 50%;">Output <input type="checkbox"/></td> <td style="width: 50%;">Input <input type="checkbox"/></td> </tr> <tr> <td>Non-Active <input type="checkbox"/> Active <input type="checkbox"/></td> <td>Type: Latch <input type="checkbox"/> Non-Latch <input type="checkbox"/></td> </tr> <tr> <td></td> <td>State: NC <input type="checkbox"/> NO <input type="checkbox"/> Supervised: <input type="checkbox"/></td> </tr> </table>		Output <input type="checkbox"/>	Input <input type="checkbox"/>	Non-Active <input type="checkbox"/> Active <input type="checkbox"/>	Type: Latch <input type="checkbox"/> Non-Latch <input type="checkbox"/>
Output <input type="checkbox"/>	Input <input type="checkbox"/>					
Non-Active <input type="checkbox"/> Active <input type="checkbox"/>	Type: Latch <input type="checkbox"/> Non-Latch <input type="checkbox"/>					
	State: NC <input type="checkbox"/> NO <input type="checkbox"/> Supervised: <input type="checkbox"/>					
Zone 8	Name = _____ Enabled <input type="checkbox"/> Assigned <input type="checkbox"/>	<input type="checkbox"/>				
	<table border="0" style="width: 100%;"> <tr> <td style="width: 50%;">Output <input type="checkbox"/></td> <td style="width: 50%;">Input <input type="checkbox"/></td> </tr> <tr> <td>Non-Active <input type="checkbox"/> Active <input type="checkbox"/></td> <td>Type: Latch <input type="checkbox"/> Non-Latch <input type="checkbox"/></td> </tr> <tr> <td></td> <td>State: NC <input type="checkbox"/> NO <input type="checkbox"/> Supervised: <input type="checkbox"/></td> </tr> </table>		Output <input type="checkbox"/>	Input <input type="checkbox"/>	Non-Active <input type="checkbox"/> Active <input type="checkbox"/>	Type: Latch <input type="checkbox"/> Non-Latch <input type="checkbox"/>
Output <input type="checkbox"/>	Input <input type="checkbox"/>					
Non-Active <input type="checkbox"/> Active <input type="checkbox"/>	Type: Latch <input type="checkbox"/> Non-Latch <input type="checkbox"/>					
	State: NC <input type="checkbox"/> NO <input type="checkbox"/> Supervised: <input type="checkbox"/>					

Form 7 Remote Display Unit (RDU) Settings

Item	Setting	✓
New Node		
Serial Number	_____	
Node Name	_____	
Remote Display Unit Connected Controller		
Controller	Serial Number: _____ Node Name: _____	<input type="checkbox"/>
Privacy Protected Display	Yes: <input type="checkbox"/> No: <input type="checkbox"/>	<input type="checkbox"/>
Alarm Filter		
External Alarm Output		
Notify through port	Port: _____ Baud rate: _____	<input type="checkbox"/>
Notifications	Notify on TIC: <input type="checkbox"/> Notify on TIF: <input type="checkbox"/>	<input type="checkbox"/>
Input Device		
Card Reader	Default = None Port selected: _____	<input type="checkbox"/>
Tag Link	Default = None Port selected: _____	<input type="checkbox"/>

Form 8 RoamAlert Server/Console PC Settings

Item	Setting	✓
Server: <input type="checkbox"/> Console: <input type="checkbox"/>		
Server/Console # _____		
Server/Console Name	_____	<input type="checkbox"/>
Tag Filters	Default = Blank Range # 1 Start: _____ End: _____ Range # 2 Start: _____ End: _____ Range # 3 Start: _____ End: _____	<input type="checkbox"/>
Tag Types	Default = All enabled Wrist: <input type="checkbox"/> Asset: <input type="checkbox"/> Staff: <input type="checkbox"/>	<input type="checkbox"/>
Suppress Missed Tag Pulse Visual and Audio Annunciation	Default = Disabled Setting = <input type="checkbox"/>	<input type="checkbox"/>
Start Up Mode Select	Default = Blank Normal Mode: <input type="checkbox"/> Secure Mode: <input type="checkbox"/>	<input type="checkbox"/>
External Alarm Output		
Notify through port	Port: _____ Baud rate: _____	<input type="checkbox"/>
Notifications	Notify on TIC: <input type="checkbox"/> Notify on TIF: <input type="checkbox"/>	<input type="checkbox"/>
Input Device		
Card Reader	Default = None Port selected: _____	<input type="checkbox"/>
Tag Link	Default = None Port selected: _____	<input type="checkbox"/>
<p>NOTE:</p> <p>Print 1 copy of the Alarm Filter (Controllers) page for every 20 controllers.</p> <p>Print 1 copy of the Alarm Filter (Receivers) page for every 20 receivers.</p> <p>Print 1 copy of the Alarm Filter (I/O-8 Modules) page for every 20 I/O-8 modules.</p>		

Form 8 RoamAlert Server/Console PC Settings (continued)

Item	Setting	✓
Alarm Filter (Controllers)		
Controller # 1 Door: <input type="checkbox"/> Elevator: <input type="checkbox"/>	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Controller # 2 Door: <input type="checkbox"/> Elevator: <input type="checkbox"/>	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Controller # 3 Door: <input type="checkbox"/> Elevator: <input type="checkbox"/>	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Controller # 4 Door: <input type="checkbox"/> Elevator: <input type="checkbox"/>	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Controller # 5 Door: <input type="checkbox"/> Elevator: <input type="checkbox"/>	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Controller # 6 Door: <input type="checkbox"/> Elevator: <input type="checkbox"/>	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Controller # 7 Door: <input type="checkbox"/> Elevator: <input type="checkbox"/>	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Controller # 8 Door: <input type="checkbox"/> Elevator: <input type="checkbox"/>	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Controller # 9 Door: <input type="checkbox"/> Elevator: <input type="checkbox"/>	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Controller # 10 Door: <input type="checkbox"/> Elevator: <input type="checkbox"/>	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Controller # 11 Door: <input type="checkbox"/> Elevator: <input type="checkbox"/>	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Controller # 12 Door: <input type="checkbox"/> Elevator: <input type="checkbox"/>	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Controller # 13 Door: <input type="checkbox"/> Elevator: <input type="checkbox"/>	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Controller # 14 Door: <input type="checkbox"/> Elevator: <input type="checkbox"/>	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Controller # 15 Door: <input type="checkbox"/> Elevator: <input type="checkbox"/>	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Controller # 16 Door: <input type="checkbox"/> Elevator: <input type="checkbox"/>	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Controller # 17 Door: <input type="checkbox"/> Elevator: <input type="checkbox"/>	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Controller # 18 Door: <input type="checkbox"/> Elevator: <input type="checkbox"/>	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Controller # 19 Door: <input type="checkbox"/> Elevator: <input type="checkbox"/>	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Controller # 20 Door: <input type="checkbox"/> Elevator: <input type="checkbox"/>	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>

Form 8 RoamAlert Server/Console PC Settings (continued)

Item	Setting	✓
Alarm Filter (Receivers)		
Receiver # 1	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Receiver # 2	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Receiver # 3	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Receiver # 4	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Receiver # 5	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Receiver # 6	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Receiver # 7	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Receiver # 8	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Receiver # 9	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Receiver # 10	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Receiver # 11	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Receiver # 12	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Receiver # 13	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Receiver # 14	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Receiver # 15	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Receiver # 16	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Receiver # 17	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Receiver # 18	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Receiver # 19	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
Receiver # 20	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>

Form 8 RoamAlert Server/Console PC Settings (continued)

Item	Setting	✓
Alarm Filter (I/O-8 Modules)		
I/O-8 Module # 1	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
I/O-8 Module # 2	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
I/O-8 Module # 3	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
I/O-8 Module # 4	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
I/O-8 Module # 5	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
I/O-8 Module # 6	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
I/O-8 Module # 7	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
I/O-8 Module # 8	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
I/O-8 Module # 9	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
I/O-8 Module # 10	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
I/O-8 Module # 11	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
I/O-8 Module # 12	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
I/O-8 Module # 13	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
I/O-8 Module # 14	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
I/O-8 Module # 15	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
I/O-8 Module # 16	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
I/O-8 Module # 17	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
I/O-8 Module # 18	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
I/O-8 Module # 19	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>
I/O-8 Module # 20	Name: _____ Can See: <input type="checkbox"/> Can Hear: <input type="checkbox"/> Can Accept: <input type="checkbox"/>	<input type="checkbox"/>

Form 9 Floor Settings

Item	Setting	✓
------	---------	---

Floor # ____ All nodes (door and elevator controllers, receivers, I/O-8 modules) placed?

New Floor Plan		
Floor Plan Name	Name = _____	<input type="checkbox"/>
Image File	Filename = _____	<input type="checkbox"/>
Position New Floor Plan		
Tabbing Order	Order = _____ (e.g., 1st, 2nd, 3rd, etc.)	<input type="checkbox"/>

Floor # ____ All nodes (door and elevator controllers, receivers, I/O-8 modules) placed?

New Floor Plan		
Floor Plan Name	Name = _____	<input type="checkbox"/>
Image File	Filename = _____	<input type="checkbox"/>
Position New Floor Plan		
Tabbing Order	Order = _____ (e.g., 1st, 2nd, 3rd, etc.)	<input type="checkbox"/>

Floor # ____ All nodes (door and elevator controllers, receivers, I/O-8 modules) placed?

New Floor Plan		
Floor Plan Name	Name = _____	<input type="checkbox"/>
Image File	Filename = _____	<input type="checkbox"/>
Position New Floor Plan		
Tabbing Order	Order = _____ (e.g., 1st, 2nd, 3rd, etc.)	<input type="checkbox"/>

Floor # ____ All nodes (door and elevator controllers, receivers, I/O-8 modules) placed?

New Floor Plan		
Floor Plan Name	Name = _____	<input type="checkbox"/>
Image File	Filename = _____	<input type="checkbox"/>
Position New Floor Plan		
Tabbing Order	Order = _____ (e.g., 1st, 2nd, 3rd, etc.)	<input type="checkbox"/>

Form 10 User Settings

Item	Setting	✓
------	---------	---

User # _____

Access Rights	User <input type="checkbox"/> Team Leader <input type="checkbox"/> Supervisor <input type="checkbox"/> Administrator <input type="checkbox"/>	<input type="checkbox"/>
Login Name & Full Name	Login: _____ Full: _____	<input type="checkbox"/>

User # _____

Access Rights	User <input type="checkbox"/> Team Leader <input type="checkbox"/> Supervisor <input type="checkbox"/> Administrator <input type="checkbox"/>	<input type="checkbox"/>
Login Name & Full Name	Login: _____ Full: _____	<input type="checkbox"/>

User # _____

Access Rights	User <input type="checkbox"/> Team Leader <input type="checkbox"/> Supervisor <input type="checkbox"/> Administrator <input type="checkbox"/>	<input type="checkbox"/>
Login Name & Full Name	Login: _____ Full: _____	<input type="checkbox"/>

User # _____

Access Rights	User <input type="checkbox"/> Team Leader <input type="checkbox"/> Supervisor <input type="checkbox"/> Administrator <input type="checkbox"/>	<input type="checkbox"/>
Login Name & Full Name	Login: _____ Full: _____	<input type="checkbox"/>

User # _____

Access Rights	User <input type="checkbox"/> Team Leader <input type="checkbox"/> Supervisor <input type="checkbox"/> Administrator <input type="checkbox"/>	<input type="checkbox"/>
Login Name & Full Name	Login: _____ Full: _____	<input type="checkbox"/>

User # _____

Access Rights	User <input type="checkbox"/> Team Leader <input type="checkbox"/> Supervisor <input type="checkbox"/> Administrator <input type="checkbox"/>	<input type="checkbox"/>
Login Name & Full Name	Login: _____ Full: _____	<input type="checkbox"/>

User # _____

Access Rights	User <input type="checkbox"/> Team Leader <input type="checkbox"/> Supervisor <input type="checkbox"/> Administrator <input type="checkbox"/>	<input type="checkbox"/>
Login Name & Full Name	Login: _____ Full: _____	<input type="checkbox"/>

User # _____

Access Rights	User <input type="checkbox"/> Team Leader <input type="checkbox"/> Supervisor <input type="checkbox"/> Administrator <input type="checkbox"/>	<input type="checkbox"/>
Login Name & Full Name	Login: _____ Full: _____	<input type="checkbox"/>

User # _____

Access Rights	User <input type="checkbox"/> Team Leader <input type="checkbox"/> Supervisor <input type="checkbox"/> Administrator <input type="checkbox"/>	<input type="checkbox"/>
Login Name & Full Name	Login: _____ Full: _____	<input type="checkbox"/>

User # _____

Access Rights	User <input type="checkbox"/> Team Leader <input type="checkbox"/> Supervisor <input type="checkbox"/> Administrator <input type="checkbox"/>	<input type="checkbox"/>
Login Name & Full Name	Login: _____ Full: _____	<input type="checkbox"/>

Form 11 Category Settings

Item	Setting	✓
Name	_____	<input type="checkbox"/>
Beacon Signal (pulse)	Yes <input type="checkbox"/> No <input type="checkbox"/> Rate (Staff or Asset): _____	<input type="checkbox"/>
Background Color	_____	<input type="checkbox"/>
Name	_____	<input type="checkbox"/>
Beacon Signal (pulse)	Yes <input type="checkbox"/> No <input type="checkbox"/> Rate (Staff or Asset): _____	<input type="checkbox"/>
Background Color	_____	<input type="checkbox"/>
Name	_____	<input type="checkbox"/>
Beacon Signal (pulse)	Yes <input type="checkbox"/> No <input type="checkbox"/> Rate (Staff or Asset): _____	<input type="checkbox"/>
Background Color	_____	<input type="checkbox"/>
Name	_____	<input type="checkbox"/>
Beacon Signal (pulse)	Yes <input type="checkbox"/> No <input type="checkbox"/> Rate (Staff or Asset): _____	<input type="checkbox"/>
Background Color	_____	<input type="checkbox"/>
Name	_____	<input type="checkbox"/>
Beacon Signal (pulse)	Yes <input type="checkbox"/> No <input type="checkbox"/> Rate (Staff or Asset): _____	<input type="checkbox"/>
Background Color	_____	<input type="checkbox"/>
Name	_____	<input type="checkbox"/>
Beacon Signal (pulse)	Yes <input type="checkbox"/> No <input type="checkbox"/> Rate (Staff or Asset): _____	<input type="checkbox"/>
Background Color	_____	<input type="checkbox"/>
Name	_____	<input type="checkbox"/>
Beacon Signal (pulse)	Yes <input type="checkbox"/> No <input type="checkbox"/> Rate (Staff or Asset): _____	<input type="checkbox"/>
Background Color	_____	<input type="checkbox"/>
Name	_____	<input type="checkbox"/>
Beacon Signal (pulse)	Yes <input type="checkbox"/> No <input type="checkbox"/> Rate (Staff or Asset): _____	<input type="checkbox"/>
Background Color	_____	<input type="checkbox"/>

Form 12 Annotation Settings

Item	Setting	✓
Annotation	_____	<input type="checkbox"/>
Annotation	_____	<input type="checkbox"/>
Annotation	_____	<input type="checkbox"/>
Annotation	_____	<input type="checkbox"/>
Annotation	_____	<input type="checkbox"/>
Annotation	_____	<input type="checkbox"/>
Annotation	_____	<input type="checkbox"/>
Annotation	_____	<input type="checkbox"/>
Annotation	_____	<input type="checkbox"/>
Annotation	_____	<input type="checkbox"/>
Annotation	_____	<input type="checkbox"/>
Annotation	_____	<input type="checkbox"/>
Annotation	_____	<input type="checkbox"/>
Annotation	_____	<input type="checkbox"/>
Annotation	_____	<input type="checkbox"/>
Annotation	_____	<input type="checkbox"/>
Annotation	_____	<input type="checkbox"/>
Annotation	_____	<input type="checkbox"/>

Form 13 Alarm Sound Settings

Item	Setting	✓
------	---------	---

Unassigned Tags

TIF (Exit) Sound File	Default <input type="checkbox"/> or File: _____	<input type="checkbox"/>
-----------------------	---	--------------------------

Wrist (resident) Tags

TIF (Exit) Sound File	Default <input type="checkbox"/> or File: _____	<input type="checkbox"/>
TLM (Pulse) Sound File	Default <input type="checkbox"/> or File: _____	<input type="checkbox"/>

Staff Tags

TIF (Exit) Sound File	Default <input type="checkbox"/> or File: _____	<input type="checkbox"/>
TLM (Pulse) Sound File	Default <input type="checkbox"/> or File: _____	<input type="checkbox"/>
TIC (Tamper) Sound File	Default <input type="checkbox"/> or File: _____	<input type="checkbox"/>

Asset Tags

TIF (Exit) Sound File	Default <input type="checkbox"/> or File: _____	<input type="checkbox"/>
TLM (Pulse) Sound File	Default <input type="checkbox"/> or File: _____	<input type="checkbox"/>
TIC (Tamper) Sound File	Default <input type="checkbox"/> or File: _____	<input type="checkbox"/>

Form 14 Messaging Device Settings

Item	Setting	✓
------	---------	---

Messaging Device Identification		
ID _____	Notes _____	<input type="checkbox"/>
Notification Events		
Notification Events	Exit <input type="checkbox"/> Off Body <input type="checkbox"/> Accept <input type="checkbox"/> Communication <input type="checkbox"/>	<input type="checkbox"/>
Events from Console	Console Name: _____	<input type="checkbox"/>

Messaging Device Identification		
ID _____	Notes _____	<input type="checkbox"/>
Notification Events		
Notification Events	Exit <input type="checkbox"/> Off Body <input type="checkbox"/> Accept <input type="checkbox"/> Communication <input type="checkbox"/>	<input type="checkbox"/>
Events from Console	Console Name: _____	<input type="checkbox"/>

Messaging Device Identification		
ID _____	Notes _____	<input type="checkbox"/>
Notification Events		
Notification Events	Exit <input type="checkbox"/> Off Body <input type="checkbox"/> Accept <input type="checkbox"/> Communication <input type="checkbox"/>	<input type="checkbox"/>
Events from Console	Console Name: _____	<input type="checkbox"/>

Messaging Device Identification		
ID _____	Notes _____	<input type="checkbox"/>
Notification Events		
Notification Events	Exit <input type="checkbox"/> Off Body <input type="checkbox"/> Accept <input type="checkbox"/> Communication <input type="checkbox"/>	<input type="checkbox"/>
Events from Console	Console Name: _____	<input type="checkbox"/>

Messaging Device Identification		
ID _____	Notes _____	<input type="checkbox"/>
Notification Events		
Notification Events	Exit <input type="checkbox"/> Off Body <input type="checkbox"/> Accept <input type="checkbox"/> Communication <input type="checkbox"/>	<input type="checkbox"/>
Events from Console	Console Name: _____	<input type="checkbox"/>

Form 15 Link Settings

Item	Setting	✓
New Link		
Link ID	_____	<input type="checkbox"/>
Link Name	_____ Disable <input type="checkbox"/>	<input type="checkbox"/>
Time Trigger (if used)		
Set Time Trigger	Set <input type="checkbox"/> Start Time _____ End Time _____	<input type="checkbox"/>
Day Selection	Mon-Sun <input type="checkbox"/> Mon-Fri <input type="checkbox"/> Sat-Sun <input type="checkbox"/> Specific Day _____	<input type="checkbox"/>
Link Trigger (I/O-8 Module) (if used)		
Logic Type	And <input type="checkbox"/> Or <input type="checkbox"/>	<input type="checkbox"/>
I/O-8 Module #1	Serial #: _____ Name: _____	<input type="checkbox"/>
Input Zone	<input type="checkbox"/> Zone #: _____ Name: _____ <input type="checkbox"/> Zone #: _____ Name: _____ <input type="checkbox"/> Zone #: _____ Name: _____ <input type="checkbox"/> Zone #: _____ Name: _____	<input type="checkbox"/>
I/O-8 Module #2 (if used)	Serial #: _____ Name: _____	<input type="checkbox"/>
Input Zone	<input type="checkbox"/> Zone #: _____ Name: _____ <input type="checkbox"/> Zone #: _____ Name: _____ <input type="checkbox"/> Zone #: _____ Name: _____ <input type="checkbox"/> Zone #: _____ Name: _____	<input type="checkbox"/>
I/O-8 Module #3 (if used)	Serial #: _____ Name: _____	<input type="checkbox"/>
Input Zone	<input type="checkbox"/> Zone #: _____ Name: _____ <input type="checkbox"/> Zone #: _____ Name: _____ <input type="checkbox"/> Zone #: _____ Name: _____ <input type="checkbox"/> Zone #: _____ Name: _____	<input type="checkbox"/>
Link Action		
I/O-8 Module	Serial #: _____ Name: _____	<input type="checkbox"/>
Output Zone	<input type="checkbox"/> Zone #: _____ Name: _____ <input type="checkbox"/> Zone #: _____ Name: _____ <input type="checkbox"/> Zone #: _____ Name: _____ <input type="checkbox"/> Zone #: _____ Name: _____	<input type="checkbox"/>

Form 16 Door Controller Hardware Settings

Door Controller Identification		✓
Ser #: _____	Name _____	<input type="checkbox"/>
Comments:		

Interface Checklist		✓
RS485 communications connected and operational		<input type="checkbox"/>
Supplied power within operational requirements of this device		<input type="checkbox"/>
Door locking interface (MAGLOCK OUT 24V) connected and operational		<input type="checkbox"/>
Door switch (DOOR SWITCH IN) connected and operational *		<input type="checkbox"/>
Forced door lock (ALARM IN) connected and operational **		<input type="checkbox"/>
Door field control (OVERRIDE IN) connected and operational ***		<input type="checkbox"/>
TIF relay (RELAY 1) connected to external device/system and operational		<input type="checkbox"/>
Aux. relay (RELAY 2) connected to external device/system and operational		<input type="checkbox"/>
<p>* One switch required per swinging door. If multiple switches are used, they must be connected in series between DOOR SWITCH IN and SYSTEM GROUND on the controller.</p> <p>** ALARM IN, if used, will force the MAGLOCK OUT 24V active. normally used to force a lockdown of one or more doors if the locking device is controlled by the door controller. The input is active when SYSTEM GROUND is applied.</p> <p>*** OVERRIDE IN can optionally be used to suspend the exciter field. Since the controller cannot detect tags while the field is suspended, caution must be exercised when configuring this option. Use of OVERRIDE IN is not recommended when door lockdown is controlled by the door controller. OVERRIDE IN can be used to suspend the exciter field until an egress attempt is made at non-locking or delayed egress equipped doors. Refer to the Installation section of the manual for details.</p>		

Hardware Configuration Parameters	Setting	✓
Total power requirements of controlled locking devices	___ Amps	<input type="checkbox"/>
Number of exciter antennas connected to this door controller	___	<input type="checkbox"/>
Exciter field range setting (measured at TP502 on door controller PCB)	___ DC Volts	<input type="checkbox"/>
Receive threshold setting for SW201 (1-9) on door controller PCB	___	<input type="checkbox"/>
Consistent tag detection range within door area *	___ Feet	<input type="checkbox"/>
Door controller operating mode (SW102 on door controller PCB)	___	<input type="checkbox"/>
Loiter alarm disabled (SW2 ON for SW 103 on door controller PCB)	<input type="checkbox"/>	<input type="checkbox"/>
<p>* Exciter field tag detection decreases gradually relative to the tag's distance from the exciter antenna(s). Tags will not consistently be detected beyond a certain range. The consistent detection range refers to the range within which tags are detected 100% of the time, regardless of the position or orientation of the tag. This is verified during exciter field tuning with the controller set to TEST MODE (Pos 0 on SW102).</p>		
Notes:		

Form 17 Elevator Controller Hardware Settings

Elevator Controller Identification		✓
Ser #: _____	Name _____	<input type="checkbox"/>
Comments:		

Interface Checklist		✓
RS485 communications connected and operational		<input type="checkbox"/>
RS485 optically isolated repeater installed on elevator segment of network		<input type="checkbox"/>
Supplied power within operational requirements of this device		<input type="checkbox"/>
Elevator controller alarm relay interfaced to elevator system (required) *		<input type="checkbox"/>
Door position switch connected and operational **		<input type="checkbox"/>
Exciter antenna(s) mounted on opposite walls, in same polar orientation		<input type="checkbox"/>
Receive antenna mounted on inner-cab ceiling		<input type="checkbox"/>
Approved travelling cable (stranded, shielded, 18AWG, 3-conductor data grade cable) installed for RS485 communications link		<input type="checkbox"/>
<p>* The elevator controller alarm relay will become active whenever a tag is detected. It should be interfaced to the elevator system so that the car will remain stationary at the floor, doors open, while the relay is active.</p> <p>** The door position switch is a dry contact elevator equipment interface, and is closed when the car doors are closed. This input suspends the exciter field after the car is underway.</p>		

Hardware Configuration Parameters	Setting	✓
Number of exciter antennas connected to this elevator controller	_____	<input type="checkbox"/>
Exciter field range setting (measured at TP502 on elevator controller PCB)*	_____ DC Volts	<input type="checkbox"/>
Receive threshold setting for SW201 (1-9) on elevator controller PCB	_____	<input type="checkbox"/>
Controller operating mode (SW102 on elevator controller PCB)	_____	<input type="checkbox"/>
<p>* The elevator controller must consistently detect all tags present within the elevator car, but detection should drop off rapidly outside the car. Tag detection inside the car must be thoroughly tested in all possible positions and orientations and verified with the elevator controller in TEST MODE (using the MODE switch (SW102) on the controller PCB).</p>		
<p>Notes:</p>		

Form 18 Receiver Hardware Settings

Receiver Identification		✓
Ser #: _____	Name _____	<input type="checkbox"/>
Location/Comments: _____		

Interface Checklist		✓
RS485 communications connected and operational		<input type="checkbox"/>
Receives tag messages from all positions and orientations within designated coverage area		<input type="checkbox"/>
Supplied power within operational requirements of this device		<input type="checkbox"/>
Receiver alarm relay interfaced to external components (NOT recommended) *		<input type="checkbox"/>
<p>* The integrated receiver alarm relay is active during all tag tamper alarm transmissions, whether activated in the RoamAlert software or not. As such, this relay may unavoidably become active during tag attachment or removal procedures. Use of this relay to annunciate tag tamper events is not recommended. Use the Alarm Output module (Part # AR2AM01-OPK) for this purpose.</p>		

Hardware Configuration Parameters	Setting	✓
		<input type="checkbox"/>
		<input type="checkbox"/>
		<input type="checkbox"/>
Notes:		

B

IMPORTING USER RECORDS

If you have a facility staff list set up outside of RoamAlert, for example in a spreadsheet or database, you can import the list into the system. The list must be in CSV (comma separated values) format, organized as shown below, with column titles spelled exactly as shown.

	A	B	C	D	E
1	Login Name	Password	Access Level	Full User Name	Pin Code
2	bfenton	fent2248	4	Barb Fenton	1998
3	mjaneway	jane1899	2	Marjorie Janeway	1867
4	hpackard	pack1546	2	Henry Packard	1546
5	dhunter	hunt5645	1	Danielle Hunter	3531
6	jmckinley	mcki1836	3	Jennifer McKinley	5789
7	mblackwell	blac2234	1	Marie Blackwell	4534
8	kparks	park9494	2	Karen Parks	8746
9	svandelay	vand4123	3	Shirley Vandelay	7691
10	dmackay	mack5698	1	Debra Mackay	8431
11	ldurno	durn4561	2	Linda Durno	4561

Access Level =	Access Group
1	User
2	Team Leader
3	Supervisor
4	Administrator
	User

Login Name	Full Name	Access Group	Status	Assigned By	Date/Time
dealer	dealer	ADMINISTRATOR	Active	sa	23/07/2001 01:18:09 PM
admin	Administrator	ADMINISTRATOR	Active	dealer	04/12/2005 10:43:14 PM
george	George Jones	TEAMLEADER	Active	dealer	20/11/2005 05:26:16 PM
taylor	Taylor Hackford	SUPERVISOR	Active	dealer	20/11/2005 05:27:20 PM
lfletch	Louise Fletcher	SUPERVISOR	Active	dealer	25/11/2005 10:34:01 AM
bfenton	Barb Fenton	ADMINISTRATOR	Active	admin	04/12/2005 10:44:20 PM
mjaneway	Marjorie Janeway	TEAMLEADER	Active	admin	04/12/2005 10:44:20 PM
hpackard	Henry Packard	TEAMLEADER	Active	admin	04/12/2005 10:44:20 PM
dhunter	Danielle Hunter	USER	Active	admin	04/12/2005 10:44:20 PM
jmckinley	Jennifer McKinley	SUPERVISOR	Active	admin	04/12/2005 10:44:20 PM
mblackwell	Marie Blackwell	USER	Active	admin	04/12/2005 10:44:20 PM
kparks	Karen Parks	TEAMLEADER	Active	admin	04/12/2005 10:44:20 PM
svandelay	Shirley Vandelay	SUPERVISOR	Active	admin	04/12/2005 10:44:20 PM
dmackay	Debra Mackay	USER	Active	admin	04/12/2005 10:44:20 PM
ldurno	Linda Durno	TEAMLEADER	Active	admin	04/12/2005 10:44:20 PM

Note that **Access Level** in the staff list corresponds to **Access Group** in the RoamAlert User list. The Access Group will be set to **User** for any staff member with a blank or a value other than 1–4 in the Access Level column.

A CSV file can be output from a variety of applications including Microsoft Excel and Microsoft Access. The top portion of the illustration above shows the staff list as an Excel worksheet. The CSV file was created using the Save As command in Excel and selecting the CSV (MS-DOS) type as the format. A line in a CSV file looks like this, with each data value separated by commas:

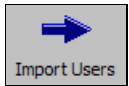
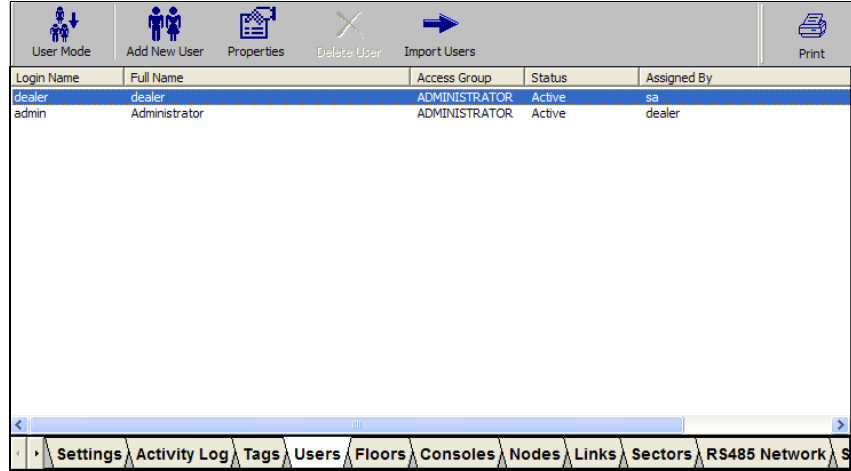
`dhunter,hunt5645,1,Danielle Hunter,3531`

Procedure: Import an External Staff List into the RoamAlert User List

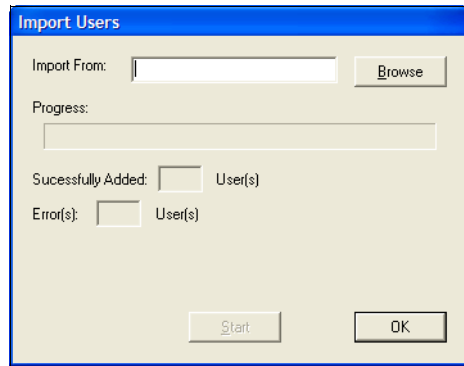
1 Prepare the facility staff list as described above and save in a folder on the RoamAlert server PC in CSV format.



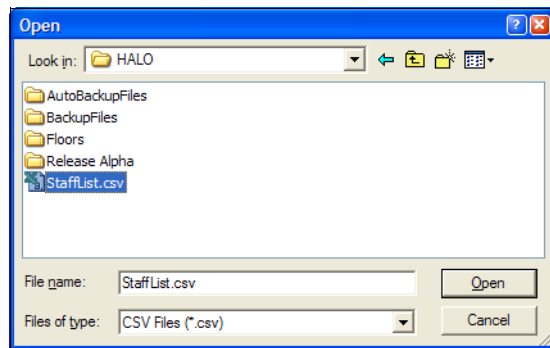
2 At the RoamAlert server in Administrator mode, select the **Users** tab.



3 Click **Import Users** on the toolbar. The **Import Users** dialog box opens.

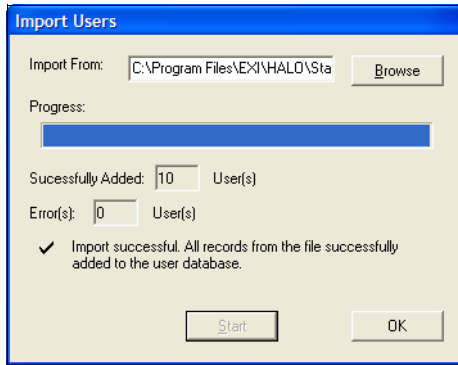


4 Click **Browse** to open the Windows File Open dialog box. The dialog box opens by default at the RoamAlert program folder.

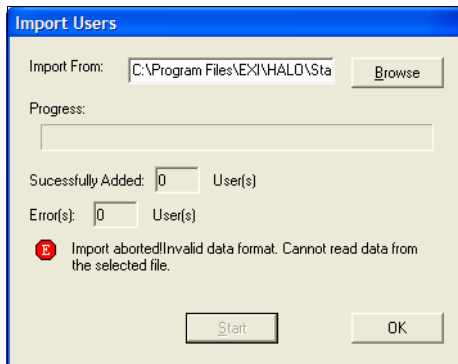


5 Select the appropriate staff list .csv file or look in other folders where you may have stored the file, select it and click **Open** to return to the Import Users dialog box.

6 Click **Start** to begin importing the selected staff list. RoamAlert shows the import progress and then displays the results.



If there is a spelling error in one or more of the column headings, RoamAlert displays this message in the Import Users dialog box.

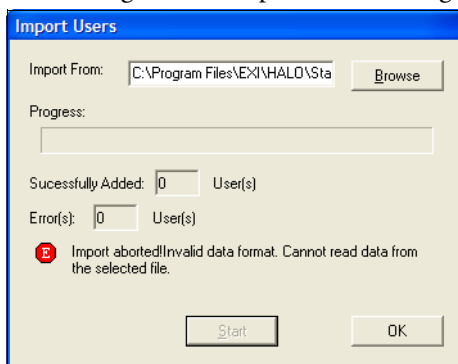


A check of the Activity Log will show this entry.

Date/Time	Type	Description
05/12/2005 12:39:39 PM	System	Import aborted! Invalid data format. Cannot read data from the selected file.

- Open the .csv file in the originating program (or Notepad), make sure the column headings are precisely correct, then try the import again.

If one or more of the users you are importing is already in the Users list, RoamAlert displays this message in the Import Users dialog box.



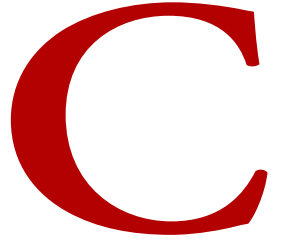
A check of the Activity Log will show this entry.

Date/Time	Type	Description
05/12/2005 12:31:19 PM	System	Automatic Import Failed (bfenton) You specified a Login Name, which is already in use by another user!

- Check the RoamAlert Users list and delete the duplicate entries or open the .csv file in the originating program (or Notepad) and delete the duplicate entries, then try the import again.

- 7 Click **OK** to close the dialog box when import is complete.
- 8 For every ten (10) users, make one photocopy of **Form 10**.
Note: *Alternately, when you have finished adding all users, you could print the user list and include it with the commissioning forms. To print the list, click the **Print** button at the upper right of the Users panel.*
- 9 In the **Setting** column of the form, record the entries you make for each setting. In the ✓ column, mark off each setting as you complete it.

A p p e n d i x



R3 RECEIVER INSTALLATION

Creating a Receiver Coverage Plan

A receiver coverage plan sets out the locations of all receivers within the RoamAlert perimeter. The density of coverage will be determined by several factors, including:

- obstacles in the physical environment,
- level of ambient RF noise, and
- client requirements for tag location (denser coverage is necessary for accurate location).

One floor of a coverage plan typically looks something like this:

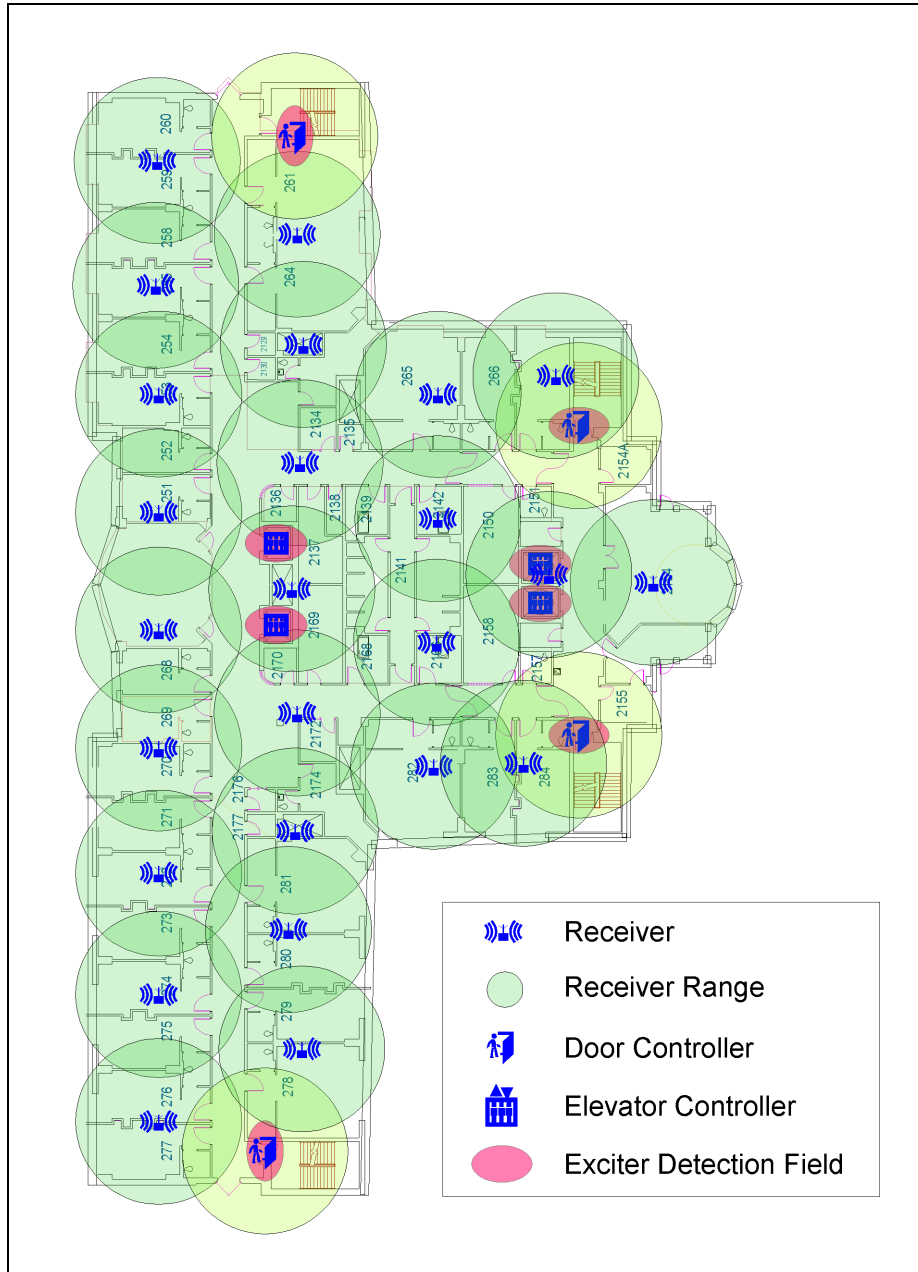


Figure C-1: Typical Preliminary Coverage Plan

You may also want to identify the locations of controllers and I/O-8 modules on the coverage plan. When you install the hardware, you will need to accurately note the controller, receiver and I/O-8 module serial numbers on the coverage plan. Later, these serial numbers will be entered into the RoamAlert software during the configuration phase (refer to the RoamAlert System Commissioning guide for software configuration details).

Locating Receivers on the Coverage Plan

As a general rule, a receiver can detect a tag within a 20 ft.(6 m) radius, or approximately 1000-1500 square feet (90-130 square meters). This coverage depends on several factors, including:

- metal barriers between the receiver and tags,
- the presence of wire glass, for example around nurseries, and
- walls, equipment and other obstacles.

Note that each door controller includes as part of its circuitry a receiver for the area around the controlled exit.

Materials Required

- Detailed facility assessment. See “Assessing the Facility” on page 2-4.
- Results of RF ambient noise testing. See “Testing for RF Noise” on page 2-6.
- Scaled floor plan (or plans) of the facility, with metal barriers, physical obstructions and noise sources indicated.
- Compass or other device for drawing scaled circles.

Procedure

Using the scaled floor plan as a guide, draw overlapping circles like those shown in Figure C-1. The center points of the circles indicate the **approximate** location for each receiver.

- 1 Based on the facility assessment and RF ambient noise testing, decide on the radius of the receiver coverage circles for your preliminary design:
 - Few metal barriers or noise sources: suggested radius 20 ft. (6 m)
 - Metal barriers and noise sources: suggested radius 15 ft. (4.5 m)
- 2 Make sure that your floor plan accurately shows all obstructions and noise sources. **Your coverage plan will be flawed if this information is not included.**
- 3 Draw the coverage pattern for all door controllers. Draw a circle with a scaled radius of 15-20 ft. (4.5-6 m) for each door controller.
- 4 Draw the coverage pattern for all corner receivers. Draw circles with a scaled radius of 15-20 ft. (4.5-6 m) in each corner of the protected area, ensuring that the radius intersects the outside corner. This makes sure that receiver coverage will extend right to the corner.
- 5 Draw the coverage patterns for the rest of the facility. Continue to draw overlapping receiver circles, until the entire facility is covered. **Do not place receivers over large metal objects or noise sources.** Shift the receiver to the side, in a location where it can be easily accessed.
- 6 In areas where there are metal obstructions or noise sources, add a receiver to ensure proper coverage. If, for example, there is a wall with wire mesh, add a receiver on the side of the wall with the weakest coverage.

Note: *This is only an approximate indication of where receivers should be located. The testing procedures in the next section may indicate that receivers need to be moved slightly to improve coverage, or that extra receivers are required in certain locations.*

Testing Receiver Coverage

To accurately evaluate RF reception and to identify the optimal placement of receivers, you should use the Technician Test Kit (**Part # AR3TK01-000**). This kit contains:

- 1 portable test receiver, with audible beeper and 9V battery,
- 1 receiver antenna,
- 1 RF test tag, and
- 1 pocket tag reader (refer to the Pocket Tag Reader User Guide for details).



Figure C-2: Technician Test Kit

The test receiver responds only to test tag messages. When the test tag button is pressed and released, the tag transmits 3 tag pulse messages. If the button is pressed and held, the tag continuously transmits 3 tag pulse messages per second. When the receiver detects the tag messages, it emits an audible tone and the RELAY LED lights.

The RADIO LED lights when RF is detected from **any source** within range near the receiver's 433.92 MHz operating frequency. This indicator helps to determine the optimal receive threshold setting. Use the **threshold switch** on the back of the receiver to set the receive range (0 = OFF, 1 = shortest, F = longest, D is the default). Some RADIO LED activity is normal, however, if the RADIO LED remains on while the test tag is not transmitting, the setting is too high.

The POWER LED should be lit steadily when the receiver is turned on and the battery is in good condition; if not, replace the battery.

Materials Required

- Detailed facility assessment. See “Assessing the Facility” on page 2-4.
- Results of RF ambient noise testing. See “Testing for RF Noise” on page 2-6.
- Scaled floor plan (or plans) of the facility, with metal barriers, physical obstructions and noise sources indicated.

- Portable test receiver, assembled with battery and antenna.
- RF test tag.

Procedure

Note: *The results of this exercise will be valid only if the test receiver is placed precisely where the permanent receiver is to be located. Metallic ceiling infrastructure such as ducts, conduits, and foil-backed tiles can impact RF characteristics.*

Using the preliminary coverage plan as a guide, test each receiver location.

- 1** Place the test receiver in each of the locations specified on the coverage plan, ensuring that the receiver is away from obstructions and noise sources, and that the antenna is oriented vertically. The receive antenna may need to protrude below the ceiling.
- 2** Press and hold the test tag button while you move throughout the area to be covered by the receiver. A steady tone from the receiver indicates good reception; an irregular tone interval indicates unreliable reception. Do not forget to test near the floor, in corners and with the tag in various orientations.
- 3** If you are not getting good reception where you think you should, adjust the receiver's range using the threshold switch, then perform Step 2 again.
- 4** Carefully plot the effective area on the coverage plan.
- 5** Discrepancies between the tested coverage and the designed coverage should be resolved at this time. Precisely mark the tested receiver location on the coverage plan, and **indicate the threshold setting**. You will use this setting when you install the permanent receiver.

A

- Alarm output module
 - installation tips, 3-42
 - installing, 3-42

C

- Central power supply
 - back-up battery, described, 1-7
 - described, 1-7
- Commissioning
 - client delivery, 5-4
 - documenting the system, 5-3
 - final system check, 5-2
- Configuration
 - add users, 4-29
 - alarm sounds, 4-45
 - annotations, 4-43
 - consoles, 4-19
 - floor plans, 4-24
 - links, 4-50
 - messaging devices, 4-48
 - node placement, 4-27
 - nodes, 4-13
 - tag categories, 4-40
 - tags, 4-32
- Connectors
 - door controller front panel, 3-6
- Controller
 - elevator, described, 1-8
- Controllers
 - door controller front panel connectors, 3-6
 - door controller installation, 3-5
 - location planning, 2-7
 - typical layouts, 2-10

D

- Door Switch
 - magnetic, described, 1-6

E

- Elevator control system
 - installation tips, 3-27
 - installing, 3-25
 - installing controller, keypad, wiring, 3-28
 - operation, 3-26
 - tuning exciter fields, 3-30
- Elevator controller
 - described, 1-8
- Exciter
 - door, described, 1-6
 - elevator, described, 1-8
 - installation tips, 3-4
 - mounting, elevators, 3-32

- tuning, doors, 3-6
- Exciter fields
 - tuning, elevators, 3-30

F

- Forms
 - alarm sounds, A-18
 - annotations, A-17
 - configuration settings, A-3
 - door controller, A-5
 - elevator controller, A-6
 - floors, A-14
 - hardware, door controller, A-21
 - hardware, elevator controller, A-22
 - hardware, R4 receiver, A-23
 - I/O-8 module, A-8, A-9
 - links, A-20
 - messaging devices, A-19
 - R4 receiver, A-7
 - server/console, A-10
 - software configuration, A-2
 - tag categories, A-16
 - users, A-15

I

- I/O-8 module
 - described, 1-9
 - installation tips, 3-38
 - installing, 3-38
- Installation Tips
 - alarm output module, 3-42
 - central power and wiring, 3-3
 - door controller, 3-4
 - elevator control system, 3-27
 - exciter, 3-4
 - general, 3-2
 - I/O-8 module, 3-38
 - keypad, 3-15
 - maglock, 3-13
 - magnetic door switch, 3-11
 - network manager, 3-54
 - R4 receivers, 3-21
 - receive antenna, 3-5
 - RS-485 network cabling, 3-3
 - Wiegand interface, 3-18

K

- Keypad
 - described, 1-6
 - installation tips, 3-15
 - installing, 3-15
 - master reset, 3-17
 - mode 2 programming, 3-16

M

- Maglock
 - installation tips, 3-13
 - installing, 3-13

N

- Network manager
 - described, 1-10
 - installation tips, 3-54
 - installing, 3-54
 - termination jumpers, 3-55

R

- Radio Frequency
 - LF interference, 2-2
 - physical barriers, 2-2
 - theory of operation, 2-2
 - VHF interference, 2-2
- Receive antenna
 - door, described, 1-6
 - elevator, described, 1-8
- Receivers
 - installing, R4, 3-21
 - R3 coverage plan, C-2
 - R3 coverage testing, C-4
 - R3 location, C-3
 - R4 installation tips, 3-21
 - R4 mounting template, 3-24
 - R4, described, 1-6
- Remote Display Unit (RDU)
 - cable assembly, 3-53
 - communicating with server, 3-52
 - installing, 3-45
 - LED displays, 3-52
 - operating modes, 3-51
 - settings, 3-47
- Repeater
 - RS-485, described, 1-8
- RoamAlert system
 - basic components, 1-4
 - minimum configuration, 2-1

- optional components, 1-8
- tags, described, 1-3
- user access, 4-5
- what it is, 1-2

S

- Server
 - alarm generation, 1-2
 - described, 1-4
- Software
 - configuring, 4-6
 - global options, 4-10
 - installation, 4-2
 - testing, 4-5
- System design
 - exit requirements, 2-5
 - facility assessment, 2-4
 - overview, 2-3
 - RF environment, 2-4
 - usability assessment, 2-5

T

- Tag reader
 - described, 1-7
- Tags
 - described, 1-3

U

- Users
 - adding new, 4-29
 - importing records, B-1
 - system access, 4-5

W

- Warranty
 - Software License Agreement, i-vi
- Wiegand interface
 - described, 1-10
 - installation tips, 3-18
 - installing, 3-18