

Safe Place® and Code Alert®

Administrator Guide – Series 10.x Software

RF TECHNOLOGIES®

Contents

Warnings / Cautions / Compliance

It is important for your facility to implement and enforce the following WARNINGS and CAUTIONS in order to keep all equipment functioning properly. Disregarding the information and instructions in this document is considered abnormal use and may result in injury or system failure.

Warnings

ACCESSORIES (SUPPLIES)—To ensure resident safety and proper operation of equipment, use only parts and accessories manufactured or recommended by RF Technologies, Inc. Parts and accessories not manufactured or recommended by RF Technologies, Inc. may not meet the requirements of the applicable safety and performance standards.

Failure to use the components and supplies specified by RF Technologies, Inc. may result in equipment and/or system failure.

EXPLOSION HAZARD—These devices should not be used in the presence of flammable gas mixtures. It should also not be used in oxygen enriched atmospheres.

INSTALLATION AND CONFIGURATION—It is the responsibility of the facility to follow the installation instructions carefully, as outlined in the applicable system guides, and to use the components and supplies specified by RF Technologies, Inc. for all installations.

Failure to use the components and supplies specified by RF Technologies, Inc. may result in equipment and/or system failure.

INSTRUCTIONS FOR SET UP AND USE—It is the responsibility of the facility to follow the instructions for set up and use carefully, as outlined in this manual, and to use the components and supplies specified by RF Technologies, Inc. for set up and use. Do not attempt to use extension cords or other equipment not supplied by RF Technologies, Inc.

Failure to use the components and supplies specified by RF Technologies, Inc. may result in equipment and/or system failure.

STATIC DISCHARGE—Do not touch the conductor portion of any conductor or port. Damage to the device may result.

STRANGULATIONS AND TRIPPING HAZARD—Due to the possibility of strangulation, all cables and cords should be routed away from the resident's throat. Cables and cords must be routed in a way to prevent tripping hazards.

SYSTEM INSPECTION—It is the responsibility of the facility to establish and facilitate a regular inspection schedule for your system. RF Technologies, Inc. recommends quarterly inspections of your system for safety and performance by a qualified RF Technologies, Inc. representative.

To arrange for a quarterly inspection by RF Technologies, Inc., call our Technical Support Department at (800)-669-9946 or (262) 790-1771.

Failure to provide regular inspection of these products may result in equipment and/or system failure.

SYSTEM MAINTENANCE AND TESTING—It is the responsibility of the facility to establish and facilitate a regular maintenance schedule for your system, as outlined in the applicable system guides. This includes regular inspection, testing, and cleaning. RF Technologies, Inc. recommends monthly maintenance and testing of your system. It is also recommended that your facility keep records of maintenance and test completions.

Failure to provide regular maintenance and testing of these products may result in equipment and/or system failure.

SYSTEM WIRING—All permanent supply connections must be done in accordance with National Electric Code, NFPA 70.

USER TRAINING—Only users who have received adequate training on the use of the system, as outlined in this manual, should use the system. It is the responsibility of the facility to ensure that all users have been trained.

Failure to adequately train employees may cause system failure due to user error. In addition, incorrect use of the equipment may also result in system failure.

MR UNSAFE

All RF Technologies transmitters, pendants and banding material “PRODUCT” have been determined to be MR Unsafe as defined by ASTM F 2503-05. Use of “PRODUCT” in a Magnetic Resonance Imaging system will cause injury to residents and staff, MR system malfunction or “PRODUCT” malfunction. Do not bring “PRODUCT” into the MR system area and follow your facility’s policies to classify and label “PRODUCT” as MR Unsafe.

Cautions

WORN OR DAMAGED PARTS—If the control unit pads or cables are worn or damaged, you must have the product serviced.

DISPOSAL—At the end of their service life the products described in this manual, as well as accessories (lithium batteries, banding material, disposable pads, etc.), must be disposed of in compliance with all applicable federal, state and local guidelines regulating the disposal of products containing potential environmental contaminants. Dispose of the packaging material by observing the applicable waste control regulations.

RESIDENT GENERATED ALARMS—Do not rely exclusively on resident generated alarms for resident care and safety. The alarm function of equipment in the possession of residents must be verified periodically and regular resident surveillance is recommended.

RESIDENT MONITORING—The most reliable method of resident monitoring combines close personal surveillance with correct operation of monitoring equipment. It is the responsibility of the facility to periodically check on residents in possession of RF Technologies, Inc.'s equipment (Pendants, Pull Cords, Control Units) to mitigate risk of inappropriate use of equipment or strangulation and stumbling hazards from cables and cords.

PRODUCT WARRANTIES—Failure to follow the Warnings and Cautions in this guide voids any and all Product Warranties.

Bio-Incompatibility Notice

Do not use Pendants with people that have sensitivities or allergies to device materials. The device materials include Acrylonitrile butadiene styrene (ABS), Silicon, Rubber, and Neoprene.

Federal Communication Commission (FCC) Compliance

FCC – Part 15

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 of the device.

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 their expense. Changes or modifications not expressly approved by RF Technologies Inc. voids the user's authority to operate the equipment.

RF Technologies FCC # **KXU-CBTX**

Radiation Exposure Statement for Mobile Devices

(For the Pull Cord model 0800-0285 and model 0800-0317; Extended Range Universal Transceiver model 0800-0388, which covers part numbers 0800-0389 and 0800-0390; Extended Range Router model 0800-0351 and model 0800-0354; Asset Transceivers model 0800-0286 and model 0800-0302 and Motion Control Unit model 0800-0415; QR Plus Pull Cord model 1200-7833; QR Plus Pull Cord with Check In model 1200-7838; QR Plus Push Button model 1200-7843; QR Plus Nurse Call Jack with Reset model 1200-7883; QR Plus Nurse Call Jack with Reset and Check In model 1200-7888)

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

Radiation Exposure Statement for Portable Devices

(For the Pendant Transceivers model 0800-0288 and model 0800-0349; Call Pendant model 0800-0375; Wander Management Transmitters model 9000-0413, model 9000-0414, model 9000-0423, model 9000-0424, model 9000-0432, model 9000-0433, model 9000-0434, model 9000-0435, model 9000-0436 and model 9000-0437; CodeWatch Transmitters model: 9000-0138, model 9000-0139, model 9000-0140, model 9000-0141, model 9000-0142 and model 9000-0143; Infant Transmitters model 9400-0066, model 9400-0262, model 9420-0066, model 9420-0262, model 9450-0066, and model 9450-0262; Patient Transmitter model 9450-4066 and model 9450-4262; Mother Transmitter model 9450-1066 and model 9450-1262; Smart Sense Transmitter model 9450-6066 and model 9450-6262; and Baby Check Transmitter model 9450-7066 and model 9450-7262)

This equipment complies with FCC and IC radiation exposure limits set forth for an uncontrolled environment. This equipment is in direct contact with the body of the user under normal operating conditions. This transceiver must not be co-located or operating in conjunction with any other antenna or transceiver.

Industry Canada Compliance

Changes or modifications not expressly approved by RF Technologies Inc. could void the user's authority to operate the equipment. The Term "IC" before the radio certification number only signifies that Industry Canada technical specifications were met.

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 of the device.

This device complies with Industry Canada license-exempt RSS standard(s). 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.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

RF Technologies IC # **2719A-CBTX**

License-Exempt RSSs

This device complies with Industry Canada's license-exempt RSSs. 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.

This page intentionally left blank

Preface

Introduction

This guide provides detailed information about the Series 10.x Software and using the software for Server Management functions, Configuration, and Defining the Client Properties. It also provides an overview of the supported systems. Refer to the Software Supported Hardware Guide (0510-0457) as well for an equipment overview.

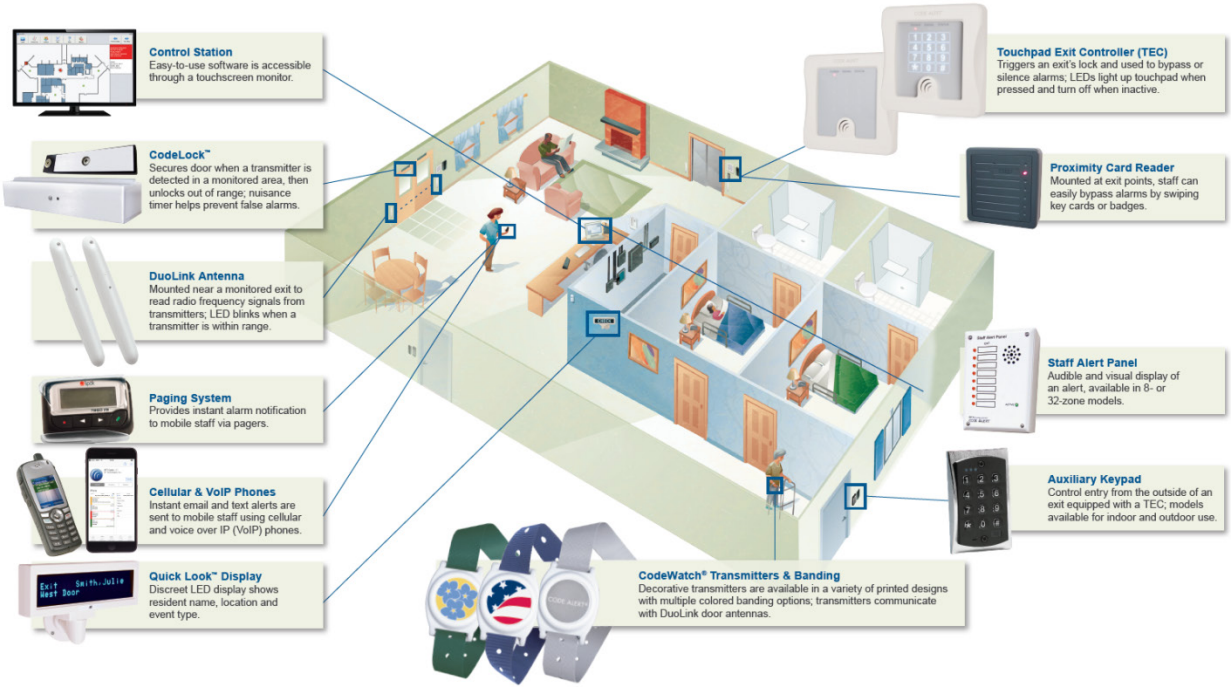
Systems Overview

The Series 10.x Software supports the following systems:

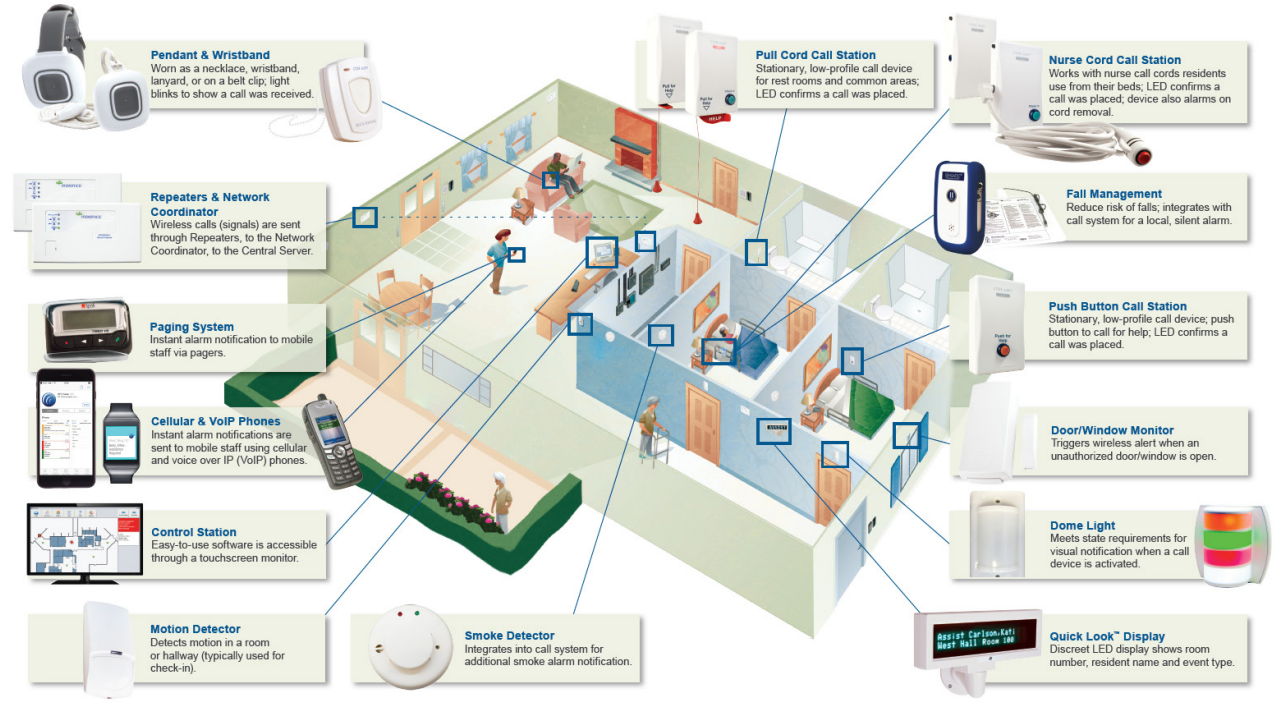
- Wander Management (9450 Series)
- Quick Response Plus
- Quick Response Premiere Wireless Call
- 9500 Series Wired Call System
- Safe Place

WARNING: These Systems are designed and intended to work in conjunction with a facility's overall security program, including reasonable operating policies and procedures. The systems, by themselves, cannot prevent abductions or elopements.

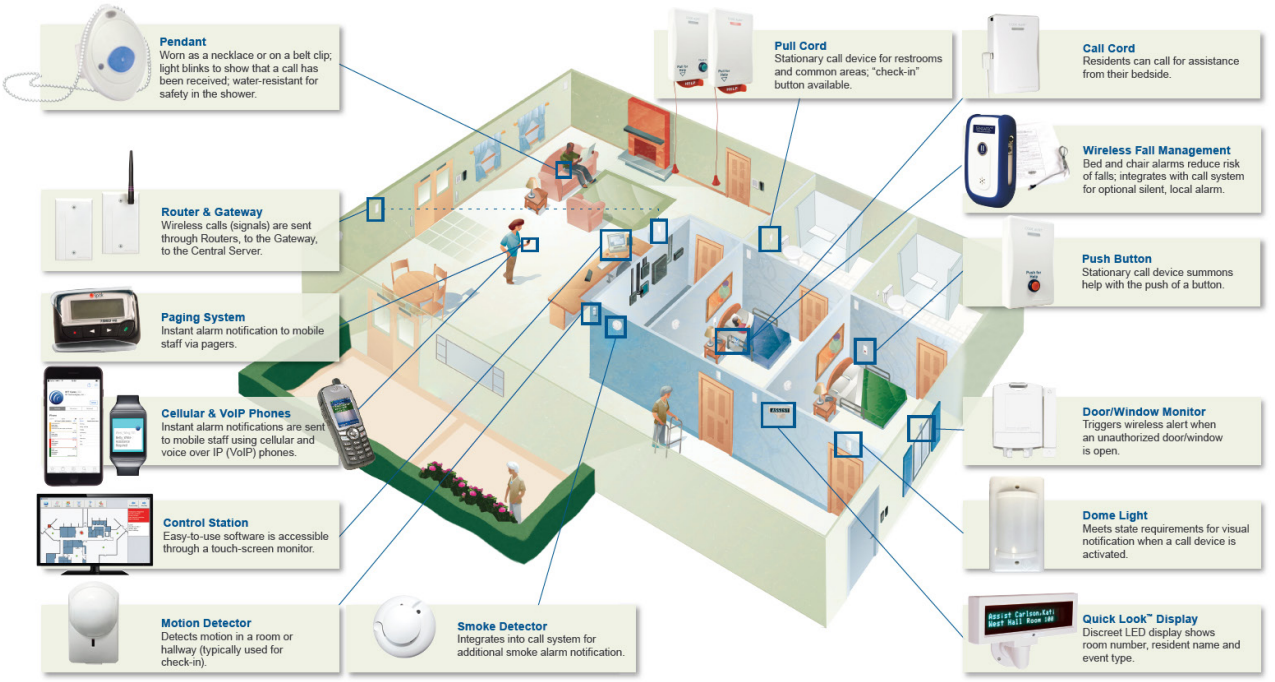
Wander Management (9450) System



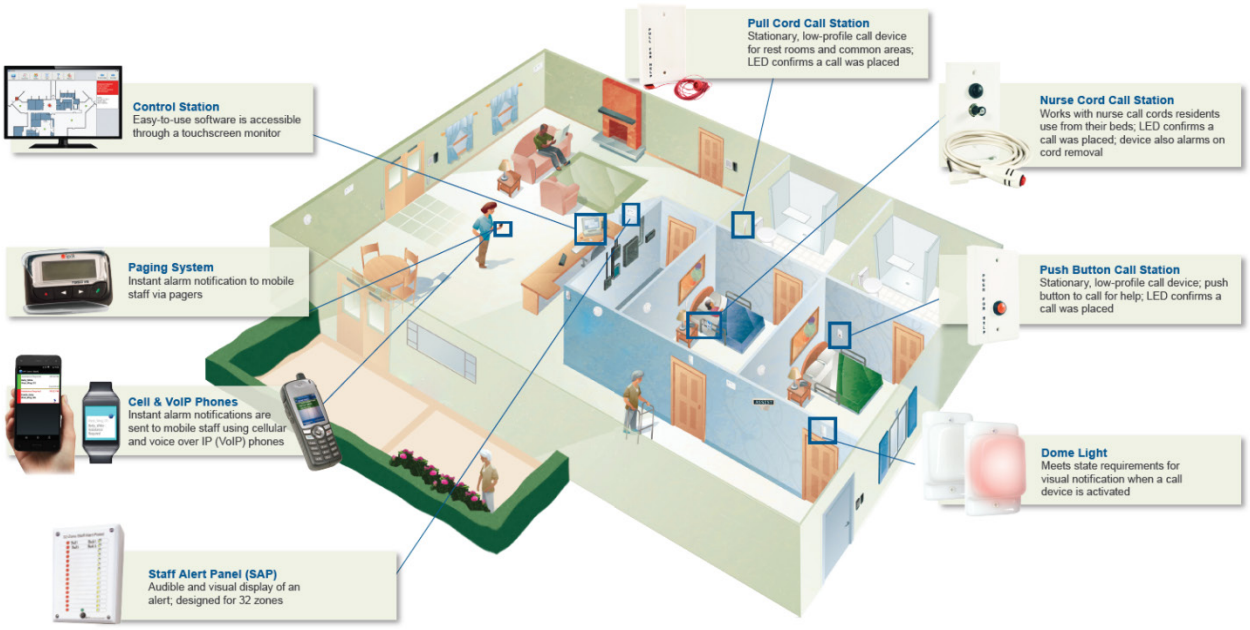
Quick Response Plus Wireless Call (QR Plus)



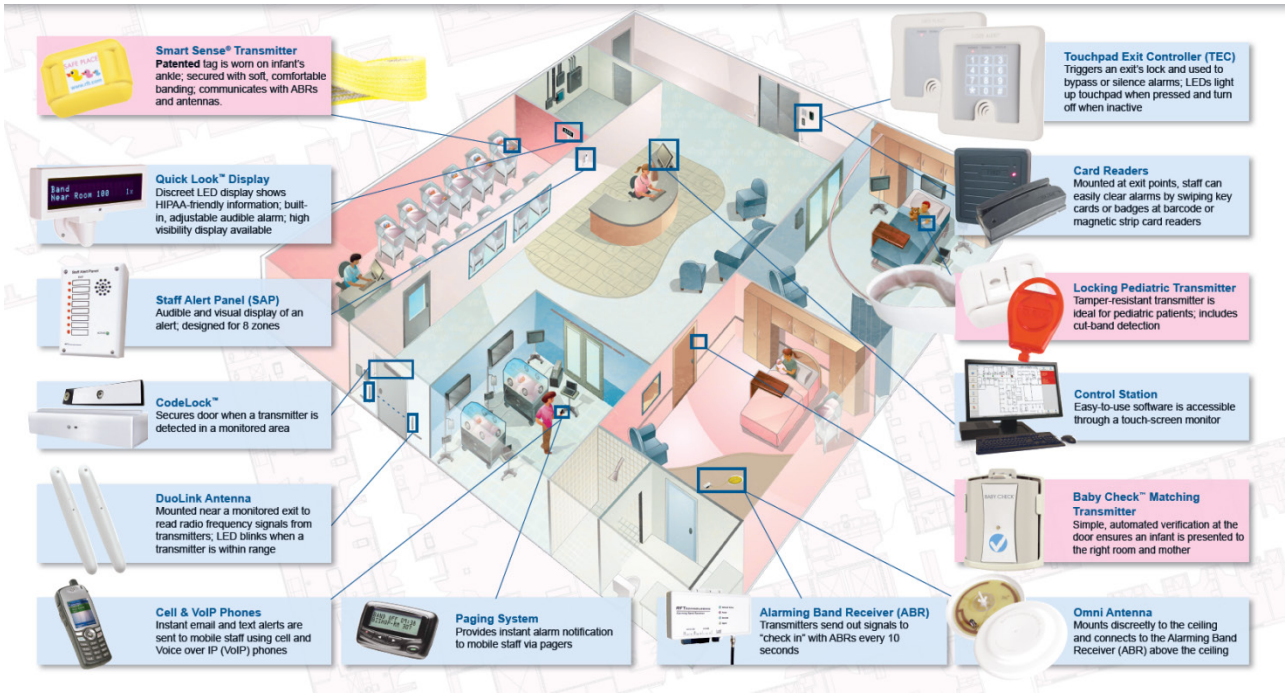
Quick Response Premiere Wireless Call (QR Premiere)



9500 Wired Call



Safe Place



Intended Audience

The Series 10.x Software Administrator Guide is intended for users who configure and administer the software. It includes detailed information about the supported systems, the software, and how to configure, administer, and maintain the software. This guide is intended to be used in conjunction with the Series 10.x Software User Guide (PN 0510-1128) along with other user and installation guides when specified.

Additional Documentation

Documentation for your system is available in Portable Document Format (PDF) on the System Documentation CD-ROM. Please contact your RF Technologies sales representative for replacement CD-ROMs.

Contact Information

For more information about RF Technologies, Inc. products, go to www.rft.com. For technical support, contact the Technical Support Team at (800) 669-9946 or (262) 790-1771. For questions or comments about the System Documentation, contact the RF Technologies Technical Publications team at techpubs@rft.com.

Product Warranty

Product Warranty information can be found on the System Documentation CD or with your original system proposal and invoice.

Chapter 1 – Initial System Configuration

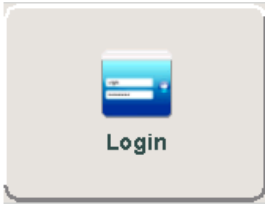
Introduction

This chapter provides details about starting the software, features of the software, and takes you through the initial steps necessary for configuring your system. The steps included are as follows:

- System Management Home Page
- Mapping COM Ports
- Getting Devices into the System
- Naming Conventions
- Location Database
- Configuring Devices
- Configuring Units
- Configuring Rooms

NOTE: After configuration changes are made to the system, it may be necessary to restart the software to ensure that the changes have been implemented. RF Technologies recommends that this is done by rebooting the Central Server. The individual RFT Windows Services should not be restarted unless directed to do so in this manual or under the direct instructions of an RF Technologies representative.

Login



1. Select **Login**
2. Enter your Login and Password or use your identification card
3. Press **Enter** or click **OK**
4. If password protection is disabled, the Main window is displayed.

NOTE: The Login, Password and Swipe Card information is case sensitive. If a “User not Authorized to perform this function” error message occurs, try turning off the Caps Lock on your keyboard.

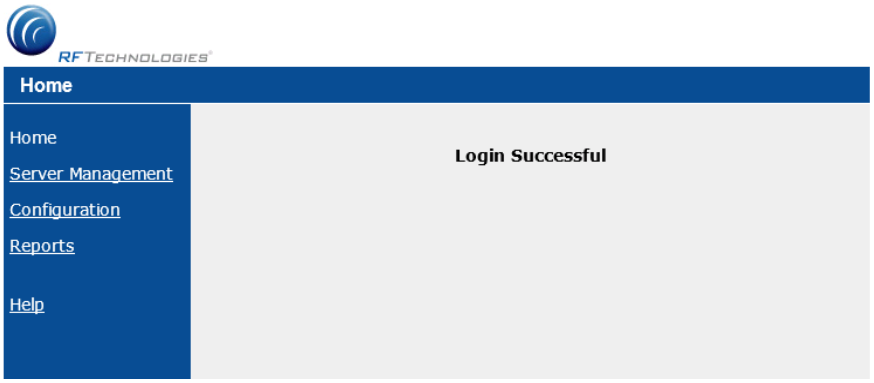
System Management Home Page

Each step in the system configuration process starts with accessing the System Management page in the software.

WARNING: The changes you make in System Management affect the entire system; you are not configuring just the Client computer, but all the Client computers at once. For instance, units are set up here and then each Client computer is configured to respond only to specified units.

To access the System Management page:

1. **Login** then select **Administrative Functions**
2. Select **Configuration**, or double-click the desktop icon if the Client application is not running
3. The System Management **Home** page opens



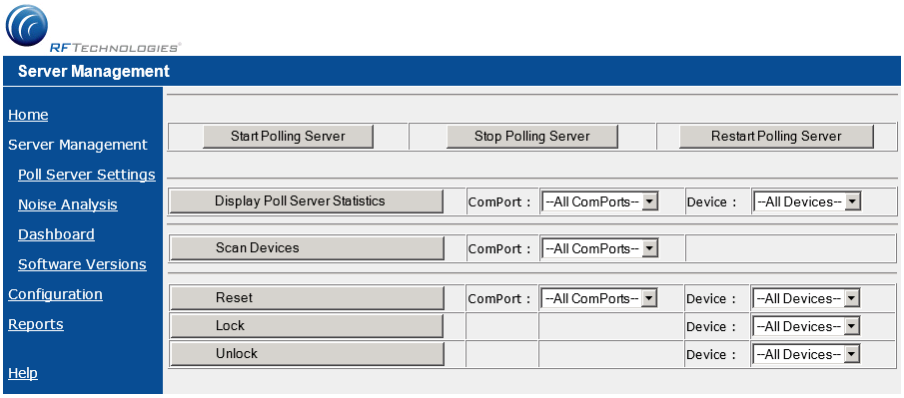
Mapping COM Ports

The Server computer is factory configured with the COM Ports to be used at your site. If it becomes necessary to modify this configuration, verify the changes with RF Technologies' Technical Support before proceeding.

Mapping the Communication Ports and Scanning Devices is done from the Server Management home page.

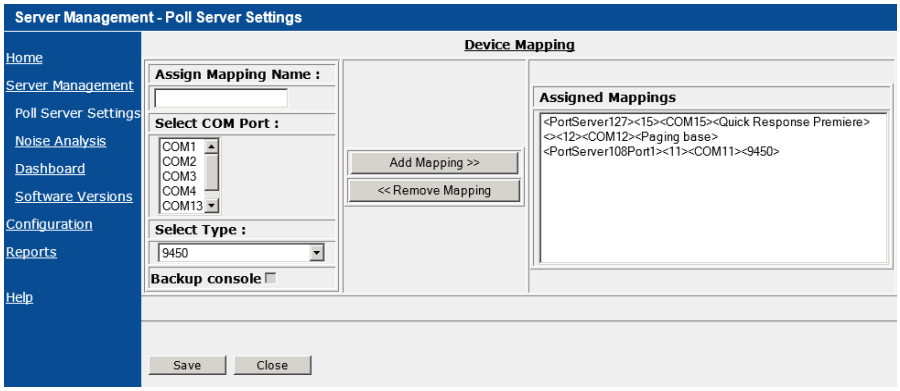
To access the Server Management page:

1. **Login** then select **Administrative Functions**
2. Select **Configuration**, or double-click the desktop icon if the Client application is not running
3. The System Management Home page opens
4. Select **Server Management**
5. The **Server Management** page opens



To map a device to a communication port:

1. Go to the **Server Management** home page
2. Select **Poll Server Settings**
3. The **Poll Server** window opens



4. In the **Assign Mapping Name** field, type in an identifying mapping name
5. Select the **COM Port**
6. In the **Select Type** pull-down, select the system type on the COM Port
7. If the COM Port type is a Quick Response COM Port, you will be given the option to select the Backup Console. The Backup Console is a unit that detects when the computer has malfunctioned/failed and provides Quick Response alarm information to the pagers
8. Select **Add Mapping** to add the setting to the **Assigned Mappings** field
9. Select **Save** to save your setting
10. Click **Close** to return to the Server Management page
11. From the Server Management page, select **Restart Polling Server**

NOTE: You must restart the Polling Server so that the system is updated with the changes that were made.

Getting Devices into the System

Before you can begin configuring the devices in the software, you must either scan them into the system or place the devices into alarm mode so that the system can establish communications with those devices.

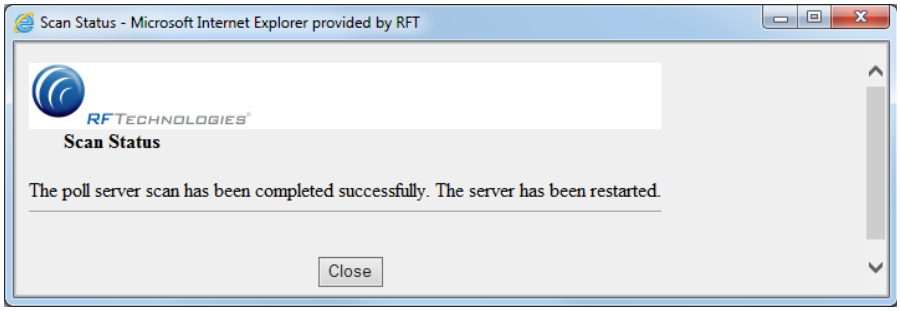
9450 System Devices

The 9450 System devices are entered into the system through the **Scan Devices** feature. Once a 9450 System device is recognized by the system, it appears in the Configuration-Devices window and can be updated.

NOTE: You must scan for devices before using the Series 10.x Software.

To scan for devices:

1. Go to the **Server Management** home page
2. Select **All Comports** from the **ComPort** pull-down
3. Select **Scan Devices**
4. The software scans for devices that have been properly configured and/or wired on the network. This scan takes about 10 seconds regardless of the number of devices in your system. Once the system is finished scanning for devices, the **Scan Status** window opens verifying the successful completion of the scan.



5. Click **Close** to close the Scan Status window and return to the Server Management home page

Quick Response Devices

Code Alert QR Plus and QR Premiere devices are entered into the system by placing the device into an alarming state.

- For QR Plus devices you must enter the individual Transmitter ID before alarming the device (see Quick Response Plus Device ID List). The system senses the device when the device goes into alarm and adds it to the device list in the Configuration-Device window. The user must then update the device information; for example, give the device a name and/or enable features.

NOTE: QR Premiere devices should check-in 3 times within the selected Supervision Time (depending on configuration). These devices will auto populate the device list when they check-in. Routers should check in every 30 seconds regardless of Supervision Time settings

Naming Conventions

It is important to name units, rooms and devices so that they clearly identify the exact location of the alarming device. RF Technologies recommends the following naming conventions based on how information is displayed on the Cisco hand-held phone and messaging devices. These recommendations should not supersede your facility's policies and procedures for naming units, rooms and devices.

Units

A unit represents a protected area in your facility that is monitored as a unit. All devices in the area are assigned to the unit, and are identified on a map or floor plan specific to the unit. RF Technologies recommends that the name of the unit begins with "Of".

- **For example:** "Of Terrance Club". This tells staff that the alarming device is of or belonging to the Terrance Club unit.

Rooms

Stationary devices such as Pull Cords and Emergency Call devices may be assigned to rooms. In this case, RF Technologies recommends that the name of the room begins with "RM" followed by the actual room number "333".

Some units may have more than one person occupying the same room. It is important when admitting a patient to a double-occupancy room that you specify which bed or side of the room the patient is assigned

- **For example:** RM101-A or RM101-B.

QR Plus Repeater

RF Technologies recommends that a Repeater is named so that it identifies its placement. The naming convention should begin with "Near".

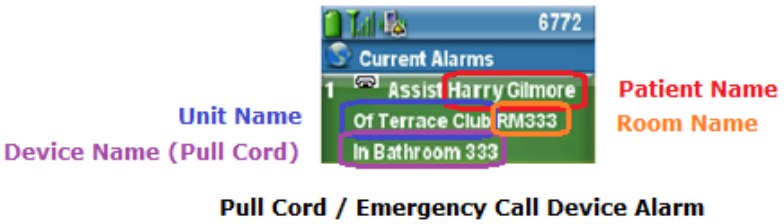
- **For example:** "Near Dining Room" or "Near 333". This tells staff that the repeater is in the Dining Room (for the first example) or near room 333.

QR Premiere Devices

RF Technologies recommends that Pull Cords, Emergency Call devices, and Routers are named to identify their placement. The naming convention should begin with "In" or "Near".

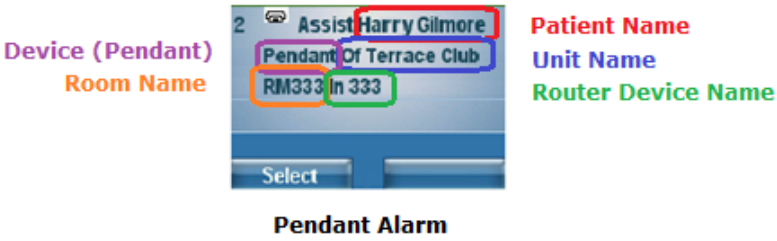
- **For example**: "In Bathroom 333" or "Near 333". This tells staff that the device is in the bathroom of room 333 or near room 333. Below is a snapshot of alarms displayed on a Cisco hand-held phone using the recommended naming conventions

Example 1



Pull Cord / Emergency Call Device Alarm

Example 2



Pendant Alarm

Location Database

Quick Response Plus optionally supports more detailed location information for Pendant events. This information is generated by a survey performed by RF Technologies Service personnel, and installed on the Code Alert/Safe Place Server. The detailed location of Pendant events is displayed on the Client, and on messages sent by outbound messaging via standard pagers, email, Cisco phone, supported smartphones, or text messaging.

NOTE: When a message is sent for an Assistance Required alarm from a QR Plus pendant, and Use Location Engine For Pendant Alarms is enabled, up to three specific locations will be displayed in the message.

- If the Location Service is not able to determine the location of the resident, the name of the Repeater with the strongest signal (the area near it) will be displayed.

If Use Location Engine For Pendant Alarms is not enabled, the name of the repeater with the strongest signal will be displayed. This location information will follow the resident's assigned room in messages sent by outbound messaging.

To install or replace the location database:

1. **Control Panel** > **Administrative Tools** > **Services**
2. Stop the **RFT Location Service**
3. Stop the **SQL Server (MSSQLSERVER)** service
4. Open **Windows Explorer** and navigate to the *Survey Profile Zip* file
5. Copy the *Survey Profile Zip* file
6. Go to the **C:\Program Files (x86)\RF Technologies\sql** directory
7. Paste the *Survey Profile Zip* file into the sql directory
8. Unzip the *Survey Profile* (double click)

9. Copy the contents (**WWSJD.mdf** and **WWSJD_log.ldf**)
10. Go back to the **C:\Program Files (x86)\RF Technologies\sql** directory and paste the contents (**WWSJD.mdf** and **WWSJD_log.ldf**) into the **sql** directory
11. When replacing an earlier location database, click **Yes** or **Yes to All** when asked if you want to overwrite the existing files
12. Restart the Server

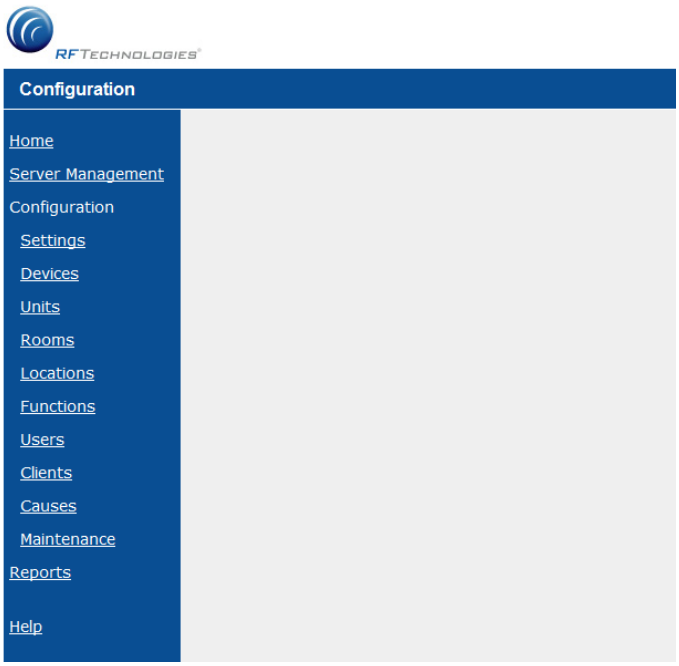
Configuring Devices

All devices recognized by the system are listed in the **Configuration Devices** window. A device that has just entered the system may not be available to use for admitting a patient until it has been configured, given a name, assigned to a unit, assigned to a room, etc.

Configuring Devices, Units, and Rooms is done from the Configuration page.

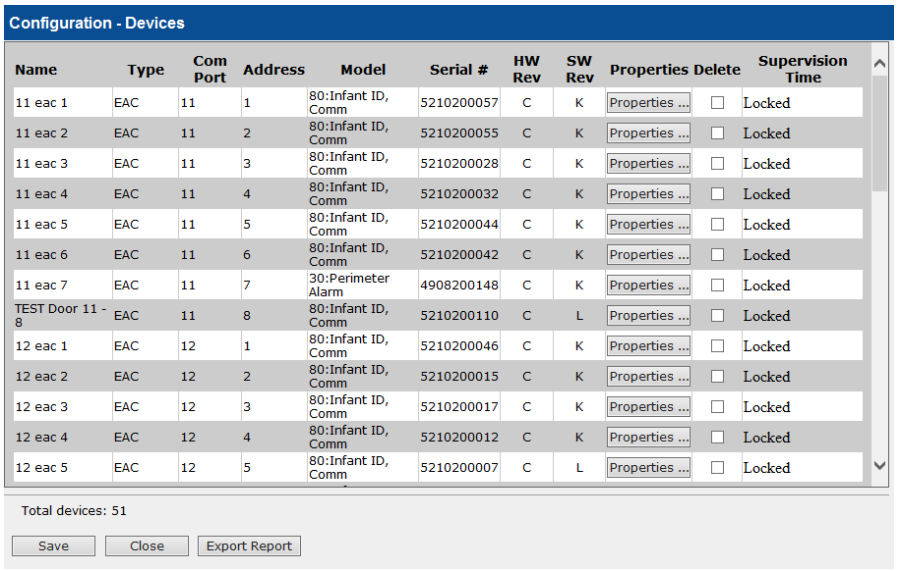
To access the Configuration Home page:

1. Select **Login** then select **Administrative Functions**
2. Select **Configuration**, or double-click the desktop icon if the Client application is not running
3. The System Management Home page opens
4. Select **Configuration**
5. The **Configuration** page opens with links to the Configuration menus



To configure a device:

1. Go to the **Configuration** home page
2. Select **Devices**
3. The **Configuration - Devices** window opens



4. Click the **Properties** button next to the device you wish to configure
5. The window that opens for configuration will depend on the device selected. An explanation on updating a Nurse Call device, a Quick Response Network Coordinator, a 9450 System device, a Quick Response Premiere device, and a 9500 Series Staff Alert Panel is found on the next few pages.
6. Click **Save**

Device Supervision Time

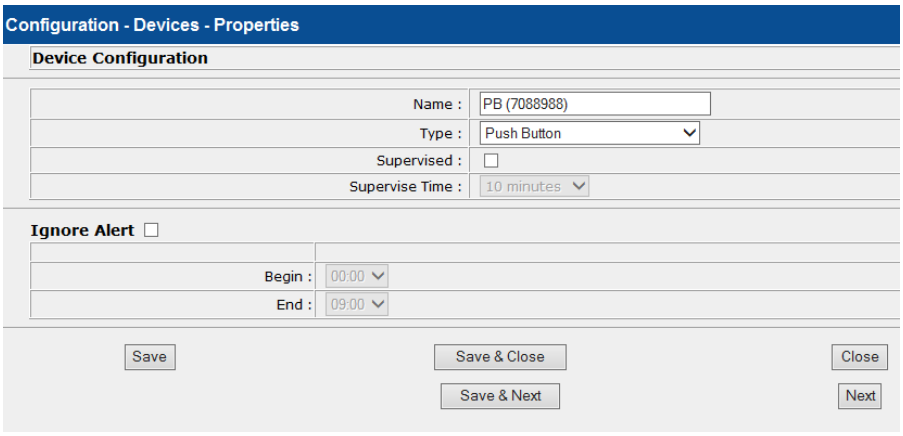
When the **Supervised** checkbox is selected, the system waits the specified amount of time before it initiates a Device Fault alarm.

The supervised time defaults to the unit's **Device Supervise Time** set during configuration. When the **Supervise Time** field is displayed, you can set specific times per device.

NOTE: A Device Fault alarm from the 9450 Quick Look Display (hardware is faulting) will post globally on all computers.

Nurse Call Devices

If the device is a Quick Response Plus device you can name the device, enable and set device supervision, select the device type from the pull-down menu, and enable and set ignore alert.

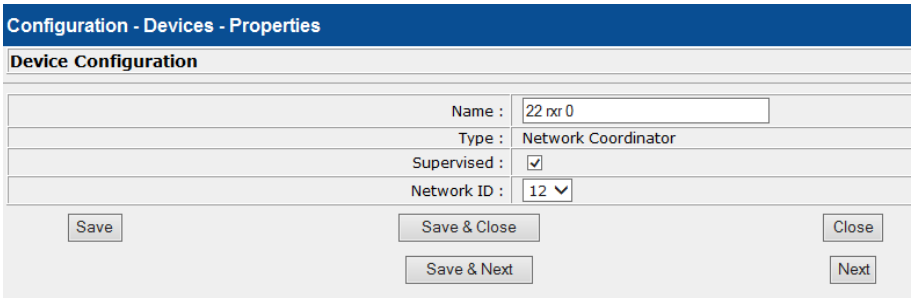


Things to Note:

- **Name:** Enter up to 20 characters maximum
- **Ignore Alert**: During the specified times, the system will not issue ANY alarms for that device. Alarms will not be displayed or sound at the Central Server, Client computer(s) or Quick Look(s).

QR Plus Network Coordinator

If the device is a Quick Response Plus Network Coordinator, you can name the device, enable device supervision, and set the Network ID.



Things to Note:

- **Name**: Enter up to 20 characters maximum
- **Network ID**: The Network ID is used for two purposes. One is to separate the facility's Repeaters from any nearby systems using similar hardware. The second is if the Network ID is set to a value other than zero, then the coordinator manages the Repeaters to improve network efficiency. (Refer to the procedure, *To verify the Network Coordinator's network ID*).

NOTE: Once the Network ID is set, all Repeaters in the Quick Response Plus Device ID List must be reset in order for the Network Coordinator to manage the network. (Refer to the procedure, *To verify each Repeater's network ID).*

To verify the Network Coordinator's network ID:

1. Restart at least the RFT SafeServe service
2. Open the Event Viewer (**Start** > **Administrative Tools** > **Event Viewer**), or right click the **Window/Start** button and select **Event Viewer**
3. Click the **plus** next to the **Windows Logs** folder
4. Select **Application**
5. Search the event log for an event after the restart of the RFT SafeServe service containing the text **InEsNcRecProto::readAndParseMessage database and NC network ID verified to be in sync. Network ID:** The end of this event will contain the Network ID of the Network Coordinator.
6. If you do not see an event with this message, but do find one with the text **InEsNcRecProto::readAndParseMessage database and NC network ID out of sync. Updating database**, open the device configuration and change the network ID to the correct value.

To verify each Repeater's network ID:

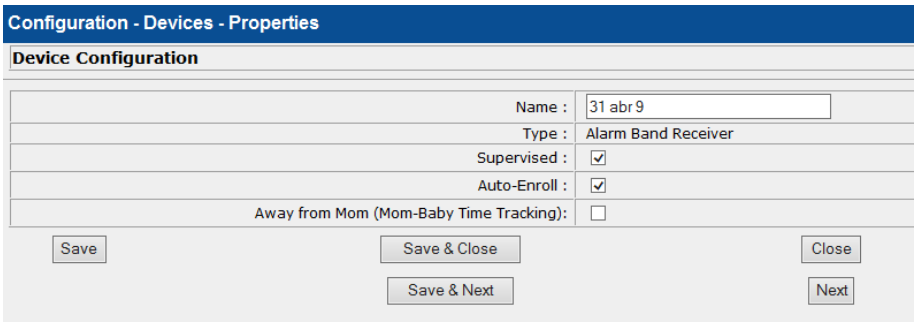
1. Go to each Repeater
2. Remove the cover and leave it off until the repeater has been verified to be in directed mode and on the correct network ID
3. Press the **reset** button
4. Open the Event Viewer (**Start** > **Administrative Tools** > **Event Viewer**), or right click the **Window/Start** button and select **Event Viewer**.
5. Click the **plus** next to the **Windows Logs** folder.
6. Select **Application**
7. Search the event log for a message in this format: **"InEsNcRecProto::readMessage network ID NID confirmed for repeater RID"**, where NID is the Network ID of the Network Coordinator, and RID is the device ID of the Repeater. If this message appears, the Repeater is configured with the correct Network ID. Continue with the next Repeater.
8. If, instead, you find a message in this format: **"InEsNcRecProto::readMessage sent network ID NID to repeater RID. Old repeater nid: NIDold"**, wait at least 10 seconds, and then press the reset button again. Continue until an event appears with the message listed in step 7.

NOTE: As the system size and number of hops increases, it may take up to 45 to 60 seconds for the message to be received by the Network Coordinator. If the reset is pressed prior to the first reset getting to the Network Coordinator, the repeater may not receive the request to change from broadcast to directed mode or get the proper network ID. If this occurs, it will require several attempts for the correct network ID to be set correctly.

9. If multiple technicians are available, have one remain at the computer viewing the events, while the others perform the steps at each Repeater.
10. Once the Repeater has been verified to be in directed mode and on the proper network ID, put the cover back onto the device.

9450 Devices

If the device is a 9450 System device, you can name the device and if applicable, enable or disable supervision and auto-enroll features.

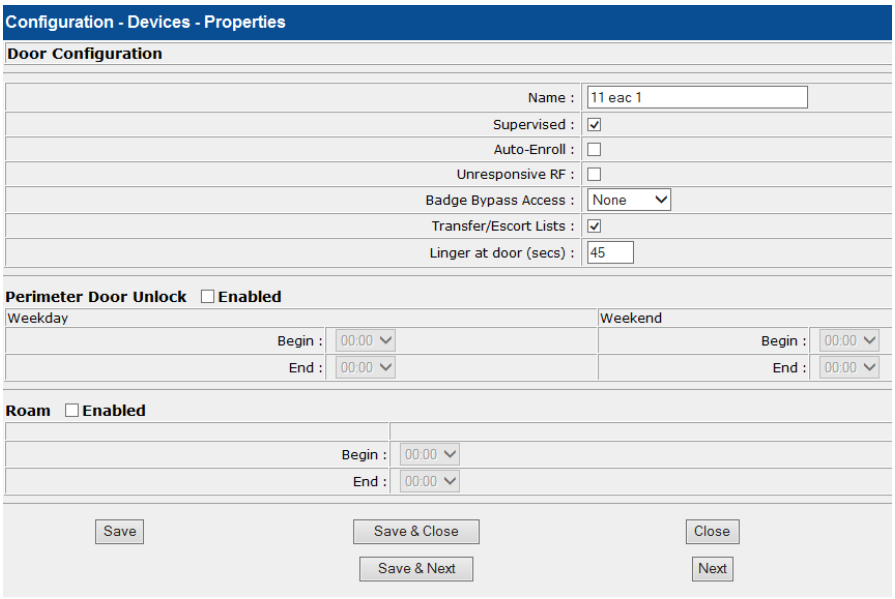


Things to Note:

- **Name**: Enter up to 20 characters maximum
- **Away from Mom (Mom-Baby Tracking)**: Applies only to Safe Place. When enabled, the alarming band receiver will be used to report the time the infant is away from its mother.

9450 Door Controller

If the device is a 9450 Door Controller, the user can name the device and if applicable, enable or disable features.

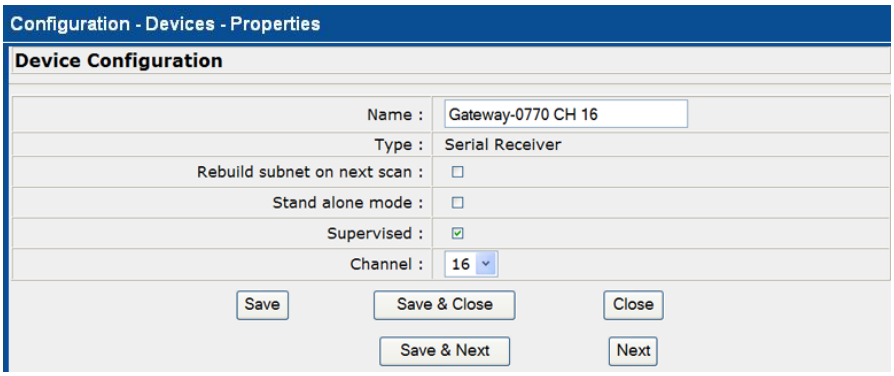


Things to Note:

- **Name**: Enter up to 30 characters maximum
- **Auto-Enroll**: Select this checkbox to enable 9450 transmitters to auto-enroll when they go into alarm at a monitored door. Transmitters enrolled using this feature will not immediately populate the Census screen.
- **Unresponsive RF:** DO NOT CHECK
- **Badge Bypass Access**: Allows the user's badge, proximity or swipe card to be used to perform a staff bypass or reset at the door. When used to perform staff bypass, the All Activities Report is populated with this event and the user who performed it.
- **Transfer/Escort Lists**: Box should be checked if this door is to be used as a transfer or escort door.
- **Linger at door**: Enter time in seconds (45-240) that:
  - the outgoing door is allowed to remain open, with the transmitter in range, before its Escort completes
  - incoming door is allowed to remain open, with the transmitter in range, before an Exit Alarm is generated for that door
  - This feature applies to 9450 transmitters only
- **Perimeter Door Unlock**: Places the door into Perimeter mode when enabled and takes it out of Perimeter mode between the times specified (begin times cannot be later than end times).
- **Roam Enable**: Allows the user to set the begin and end times for permanent bypass mode, that is when doors are open and persons can go through without triggering an alarm (begin times cannot be later than end times).

QR Premiere Gateway

If the device is a Quick Response Premiere Series Gateway, you can name the device, enable and set device supervision, and choose the channel selection for the Gateway (25 is the default).



Things to Note:

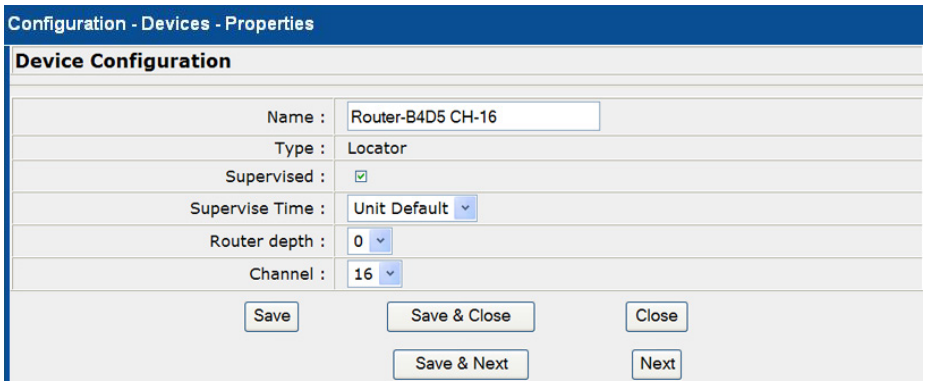
- **Rebuild subnet on next scan**: DO NOT CHECK

WARNING: Rebuilding the subnet should only be done when end devices are not present during installation. During the Rebuild, the system will be down for up to 10 minutes.

- **Stand alone mode**: DO NOT CHECK
- **Channel**: Channel selection is site specific and dependent on the site's environmental issues.

QR Premiere Router

If the device is a Quick Response Premiere Router, you can name the device, enable and set device supervision, and choose the channel selection for the Router (25 is the default).



Things to Note:

- **Name**: Enter up to 20 characters maximum
- **Router depth**: The Router Depth option allows you to adjust Router Depth by staggering 5-second Router resets by one, two, three or four minutes. Each Router has an association limit of 6 Routers; the hop limit for each Router is 4.

- **Channel**: Channel selection is site specific and dependent on the site's environmental issues. Ensure that the channel selected is a channel assigned to one of the Quick Response Premiere Gateway devices.

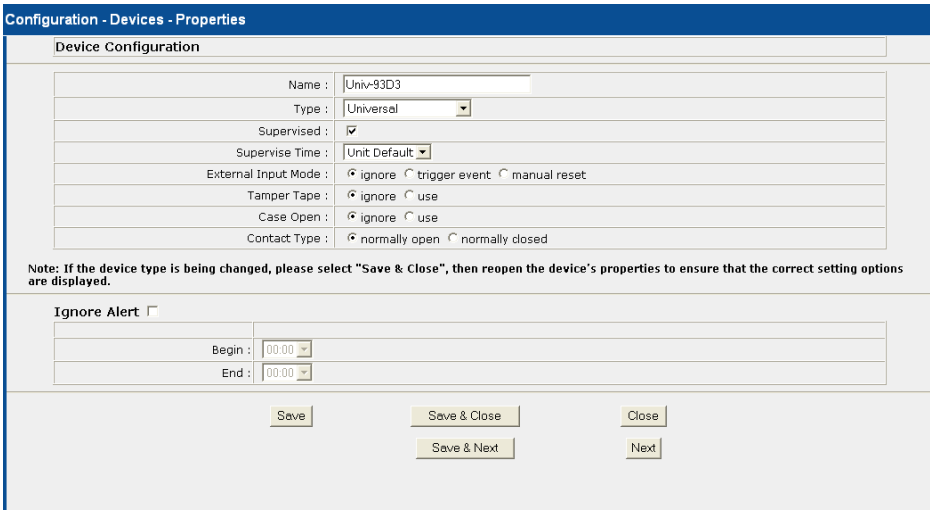
CAUTION: If a router is assigned to a channel without a gateway, the router will not be able to communicate with the server.

To correct this issue:

1. Configure a gateway for channel 25
2. Scan the COM port for the gateway
3. Physically reset the router to use the default channel (25), and wait for it to check in
4. Reconfigure the gateway to the correct channel
5. Reconfigure the router to the correct channel
6. Scan the COM port for the gateway

QR Premiere Universal Transceiver

The Quick Response Premiere Universal Transceiver is used for custom applications. If the device is a Universal transceiver you can name the device, enable and set device supervision, select the device type from the pull-down menu, and enable and set ignore alert. Additionally, you can configure the External Input Mode, Case Open and Contact Type.

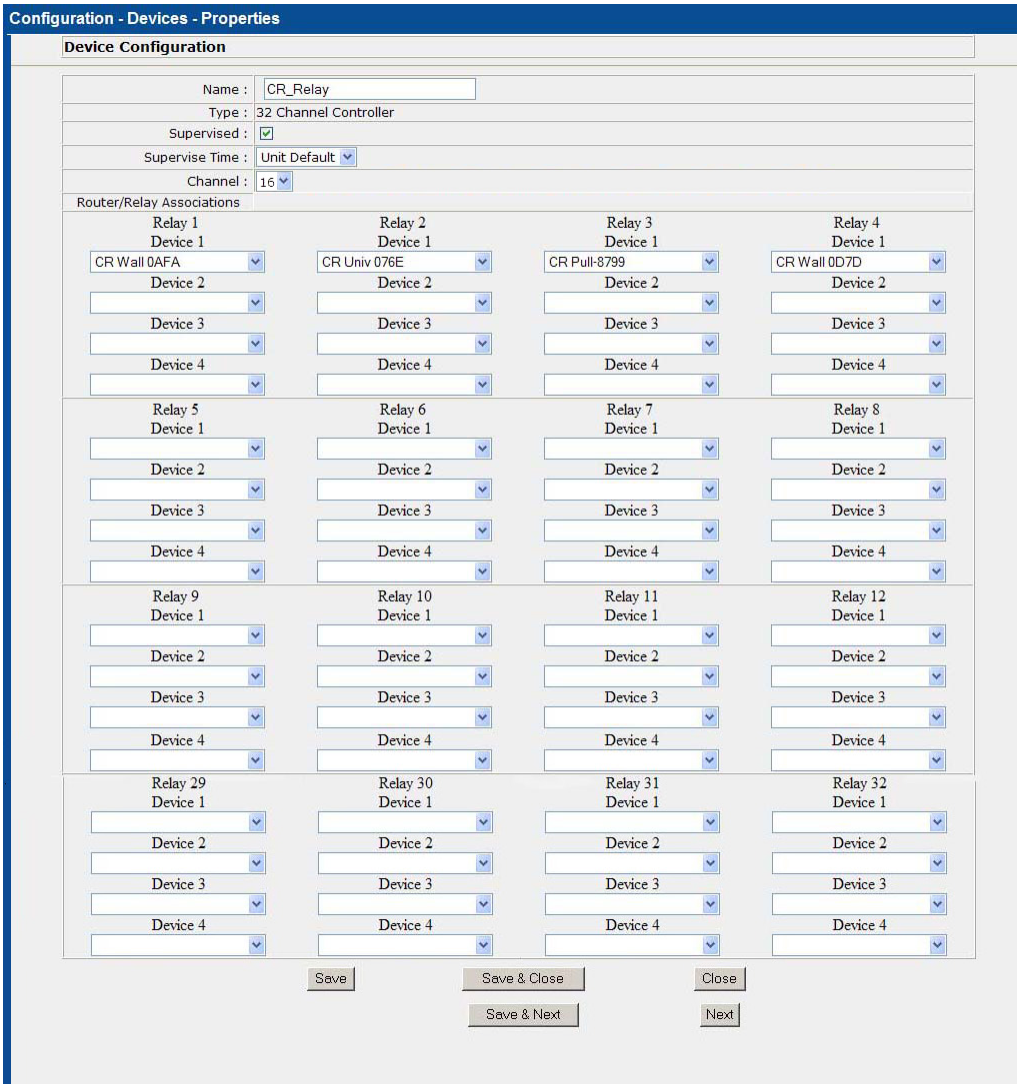


Things to Note:

- **Name**: Enter up to 20 characters maximum
- **State Changes**: You can choose how the system handles a state change when a device is opened or closed (ignore, trigger an event, manually reset, etc…) for external input, tamper, case, and contact type.
- **Ignore Alert**: During the specified times, the system will not issue ANY alarms for that device. Alarms will not be displayed or sounded at the Central Server, Client computer(s) or Quick Look(s).

QR Premiere 32 Channel Controller

If the device is a Quick Response Premiere 32 Channel Controller device you can name the device, enable and set device supervision, set the Router depth, change channels (25 is the default), and configure the Router/Relay Association.



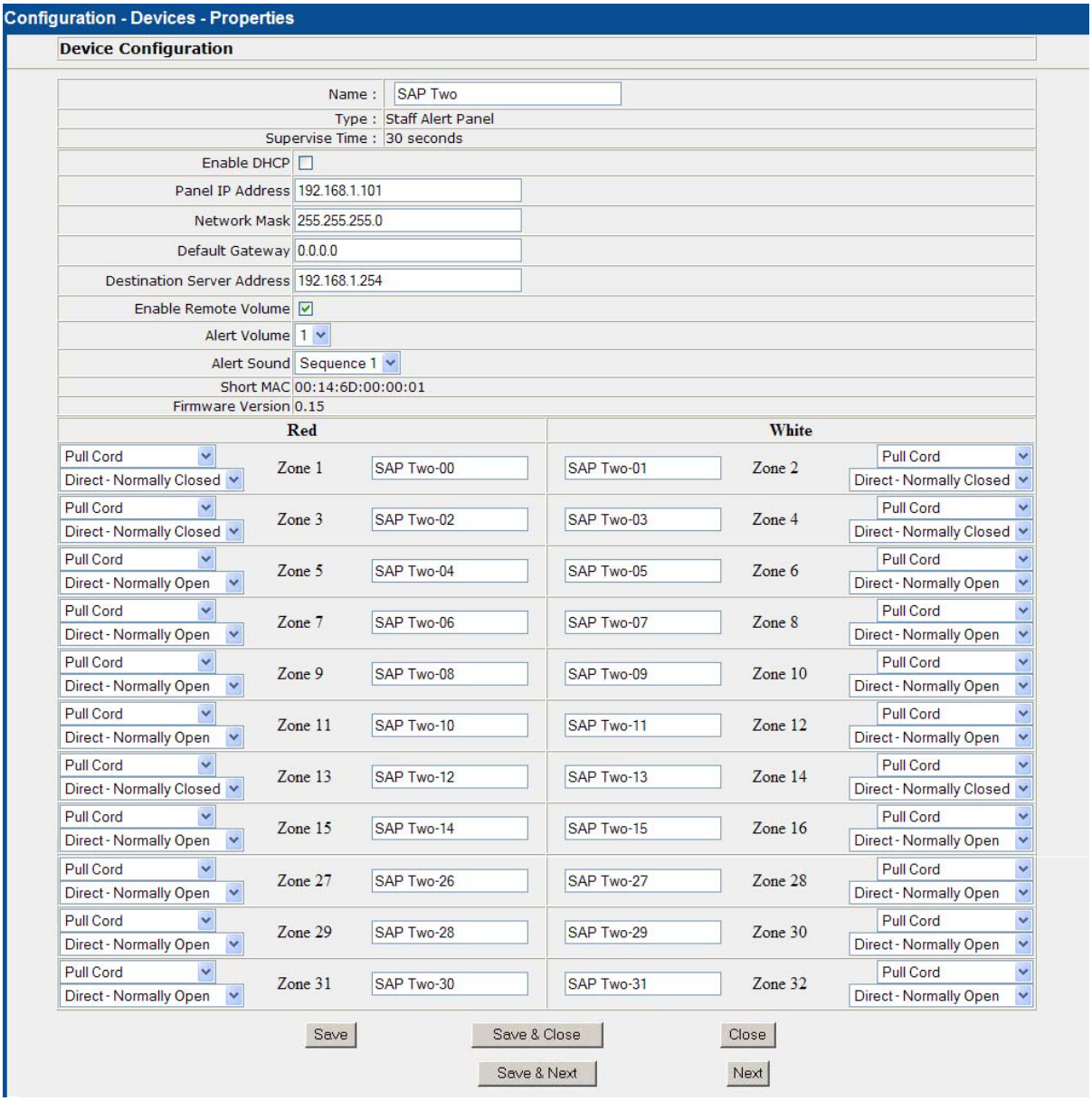
Things to Note:

- **Name**: Enter up to 20 characters maximum
- **Router/Relay Association**: There are 32 relays with each relay capable of monitoring four devices.
  - The Dome Light is triggered if any of the devices associated with that relay goes in alarm.
  - Devices selected must be from the same unit as the 32 Channel Controller.

9500 Series 32 Zone Staff Alert Panel

If the device is a 9500 Series 32 Zone Staff Alert Panel (SAP) you can name the device, enable remote volume and configure each zone with a device, its name, type and option settings. Each SAP is displayed in the device list as 33 separate devices, the SAP and 32 Zones. Only the SAP can be deleted; its zones cannot be deleted separately.

If the SAP is alone on the network with the server, the values displayed for address, mask, and gateway can be left alone. If shared with other systems, ask the network administrator for these values. If the network contains only the server and multiple SAPs, assign a separate IP address to each SAP.

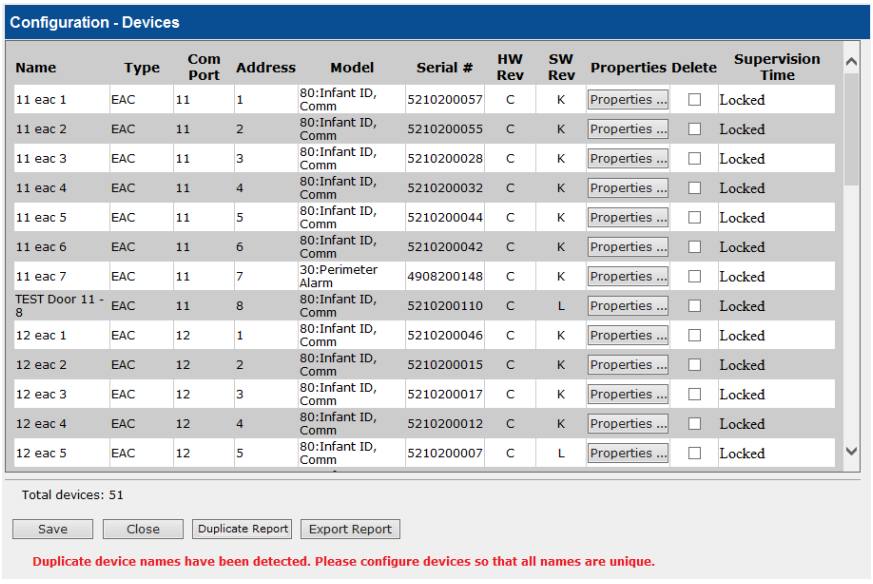


Things to Note:

- **Name**: Enter up to 20 characters maximum
- **Enable DHCP**: Only enable the DHCP if the SAP is on a network with a DHCP server. If you enable the DHCP and there is no DHCP Server, you will have to physically restore the SAP's factory default settings.
- **Destination Server Address**: The address of the server running the Series 10.x Software.
- **Enable Remote Volume**: Allows you to configure the volume level for the SAP remotely at the computer, instead of locally at the SAP.
- **Zones**: There are 32 Zones for each SAP. Each zone can be configured for device type, option setting, and zone name.
  - **Zone Name:** Enter up to 15 characters maximum
  - **Device Type:** The device type determines the type of alarm generated (for example, a Pull Cord generates an Assistance Required alarm).
  - **Option Setting:** The option setting determines if the connection is coming via the dome light or directly to the SAP. If the connection is coming from the Dome light, the SAP is capable of generating three event types; alarm, reset and tamper.

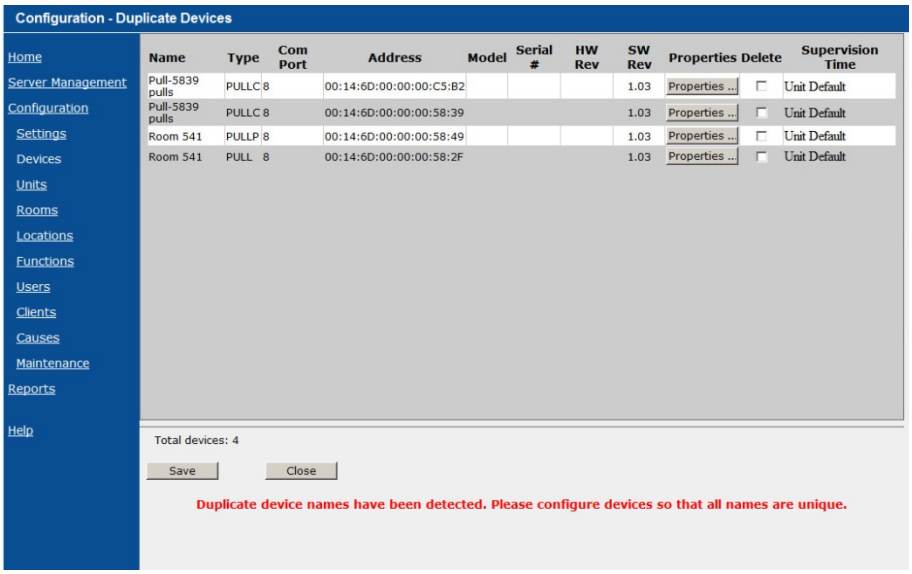
Duplicate Devices

When there are duplicated devices in the system, a message **Duplicate device names have been detected. Please configure devices so that names are unique** and a Duplicate Report button appears at the bottom of the Configuration Devices window.



To resolve the duplicate device:

1. Select **Duplicate Report**, the **Configuration - Duplicate Devices** window opens



2. If the device is no longer in the system and you wish to remove it, click the **Delete** checkbox next to the device you wish to remove, then click **Save**
3. If you wish to rename the device, click the **Properties**... box next to the device you wish to rename
4. In the **Name** field, enter the new name of the device
5. Click **Save** to save changes

Export Devices

The user can export a list of importable Devices to use as needed. To export a list of Quick Response Plus devices, your system must be licensed for Quick Response Plus and Smart ID and must be running the Series 10.x Software or later.

To Create a List of Devices:

1. Select **Export Report**
2. The **File Download** prompt will open asking you if you want to open or save this file
3. Select **Save** and the **Save As** window opens for you to save your file
4. Navigate to the folder you wish to save the file. The file is saved as a .**csv** file
5. In the **File Name** text box, rename the file or use the default name

   Select **Save**

Removing a Device

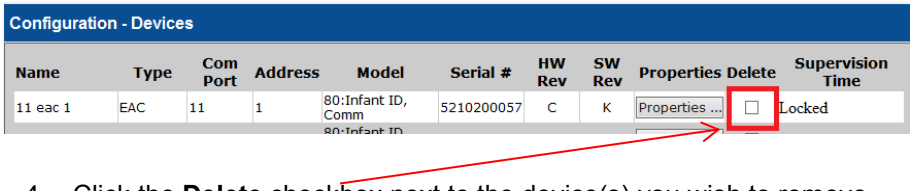
Devices assigned to a unit and a room must be removed from the unit and room before they can be deleted from the system.

A 9450 device must be removed from the network and **in** Device Fault before it can be deleted from the system.

A 9500 Staff Assist Panel (SAP) must be removed from the network or powered off, and the SAP and all 32 inputs in communication fault, before it can be deleted from the system.

To remove a device:

1. Go to the Configuration home page
2. Select **Devices**
3. The **Configuration Devices** window opens



4. Click the **Delete** checkbox next to the device(s) you wish to remove
5. Click **Save** to delete the selected devices
6. You must restart the Client application to clear devices from the Map view and alarms from the Event list

Configuring Units

When each device installed in your facility has been added to the software database, units must be defined and added. Units help the staff to ensure that each patient is accounted for in the system. Upon admission, a patient must be assigned to a Unit.

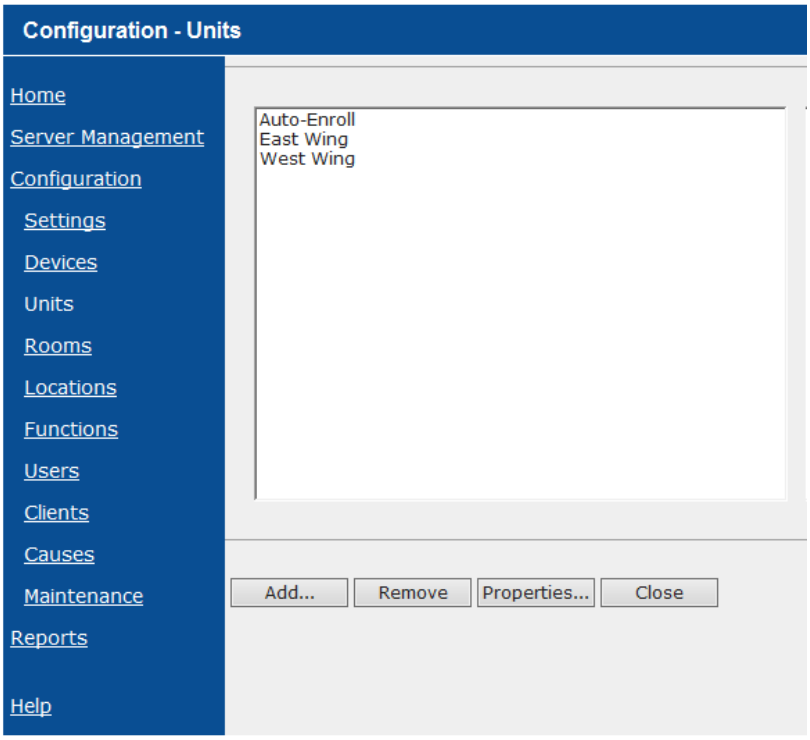
A Unit represents a protected area in your facility that will be monitored as a unit, such as the nursery or intensive care. All devices in the area are assigned to the unit, and are identified on a map or floor plan specific to the unit. If an alarm occurs, the relevant alarm information, such as the patient's name, the type of event, and the location of the event, is displayed at any Client that has been configured to monitor the unit.

Some System Properties, such as the device supervision interval and time allowed for the discharge and adjust functions, are also defined at the unit level.

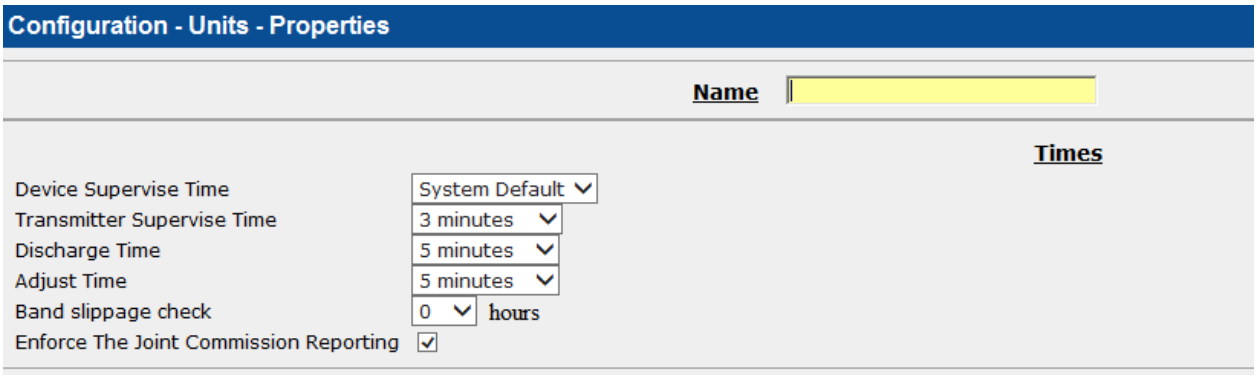
Adding a Unit

To add a unit:

1. Go to the **Configuration** home page
2. Select **Units**
3. The **Configuration - Units** window opens



4. Select **Add**
5. The **Configuration – Units - Properties** window opens



- **Name:** Unit names can only contain alphabetic and numeric characters, spaces, and the following special characters: **! - _ . ; [ ]{ }( )**

NOTE: The Unit and Room name field is limited on the Quick Look Display. The combined name length should not exceed 20 characters. The room number will be truncated should the combined characters exceed this limit. If this happens, the patient's room number will need to be verified in the Event Information window.

The Quick Look Display is a secondary means of alarm notification. For more specific patient or asset alarm information and location, reference the Client application.

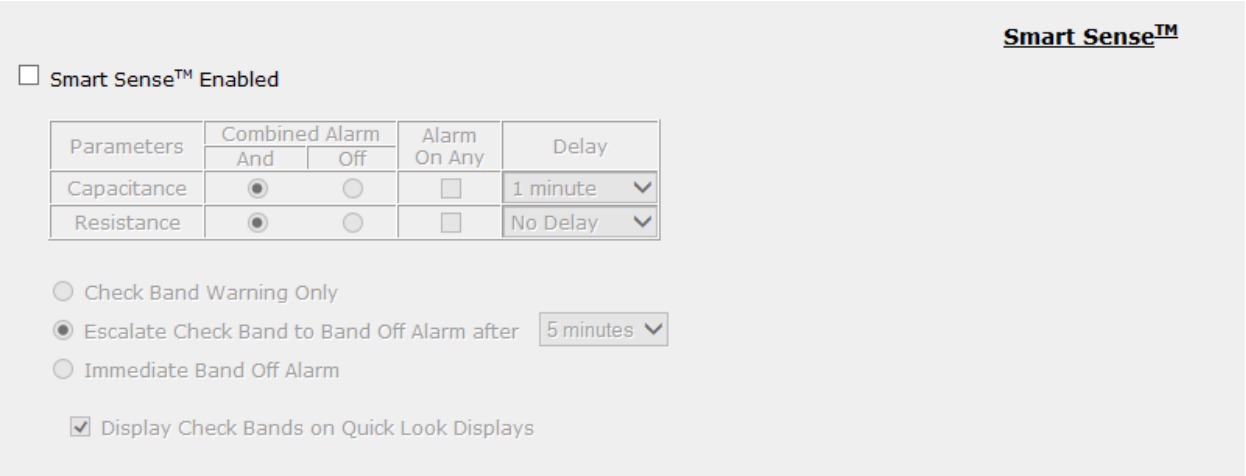
Times From the Times section of the window, the following options are available:

- **Device Supervise Time:** The number of minutes/hours that the system should wait before it initiates a Device Fault alarm for Quick Response Plus and Quick Response Premiere devices.
  - For Quick Response Plus devices, the amount of time selected must be 4 hours and above
  - For Quick Response Premiere (UL 1069) devices, the amount of time selected must be either 88, 89, or 90 seconds
- **Transmitter Supervise Time:** The number of minutes/hours that the system should wait before it initiates a No Signal alarm for a 9450 transmitter and Quick Response Premiere pendants.

  Five minutes is selected by default for Safe Place Systems. For Code Alert Systems, 24 hours is selected by default. Quick Response Plus pendants have a fixed supervision period of 4 hours.

NOTE: Setting the device and transmitter supervision times to OFF will disable supervision and detection of a low battery condition. This setting is only to be used temporarily for troubleshooting purposes.

- **Discharge Time:** The number of minutes allowed for removing the banding material from an alarming band transmitter in order to discharge a patient. **Five minutes is selected by default.**
  - If the selected number of minutes passes and the banding material is not removed, the system notifies the user of a "Discharge Expired" alarm condition. If the Unit does not have Alarming Band Receivers, an immediate Discharge will be initiated.
- **Adjust Time:** The number of minutes allowed for adjusting the banding material on a transmitter. **Five minutes is selected by default.**
  - If the selected number of minutes passes and the banding material is not replaced, the system notifies the user of an "Adjust Expired" alarm condition.
- **Band slippage check:** The number of hours allowed to elapse, after admission, before an alarm is issued to remind staff to check the banding material on a transmitter for band slippage. Band slippage check is not a feature for Asset or Mother transmitters. **Default is 0.**
- **Enforce The Joint Commission Reporting:** If the Enforce The Joint Commission Reporting feature is activated, you must select an Event Cause once the alarming device has been reset. When you reset the alarming device, the Red Alarm changes to a White Alarm in the Alarm Message Box. **This is checked on by default.**



Smart Sense From the Smart Sense section, the following options are available:

- **Smart Sense Enable/disable:** When disabled, the system will only recognize Cut Band alarms. When enabled, there are two parameters for you to choose the criteria for generating a Band Off or a Check Band alarm.
  - **Capacitance**: Change in contact between transmitter and infant. **Default is 1 minute.**
  - **Resistance**: No motion detected from the banding material (that is, the band is no longer stretching with normal infant movement). **Default is No Delay.**
    - Select any valid combination of **Combined Alarm** radio buttons and the **Alarm on Any** checkboxes.
    - Click the **OFF** radio button next to a parameter to select it as a parameter that will not be used for determining a Band Off alarm.
    - Click the **Alarm On Any** checkbox next to a parameter to individually choose it to generate a Band Off alarm.
    - **Delay:** Settings can also be changed for each parameter. Once a Band Off condition is met, the alarm will be delayed for the configured time. If the Band Off condition resolves within the delayed time, the Band Off alarm will not be sent. For Combined Alarms, the parameter with the longest delay takes precedence.

NOTE: Smart Sense transmitters will not follow the settings of an Auto-Enroll Unit but will adopt the settings of the Unit they are being assigned to. Smart Sense transmitters admitted and set to follow the Unit's Smart Sense settings will retain their original settings when the Unit's Smart Sense configuration is changed.

- **Check Band Warning Only:** When selected, only a Yellow Check Band alarm will be generated. The alarm will not escalate to a red Band Off alarm.
- **Escalate Check Band to Band Off Alarm:** The number of minutes the system should wait before it escalates a Check Band alarm to a Band Off alarm. **This option is selected by default with alarm after 5 minutes**.
- **Immediate Band Off Alarm:** Select this option if you do not wish to receive a Check Band alarm when a Smart Sense alarm is generated.
- **Display Check Bands on Quick Look Displays:** Displays Check Band alarms on the Quick Look display for Smart Sense transmitters assigned to the Unit. This option is enabled if Smart Sense is enabled and Immediate Band Off Alarm is not selected. **By default, this setting is checked.**
  - For enrolled transmitters, the Check Band warning will still only appear on Quick Look displays in the patient's Unit. Check Band alarms for Auto-enrolled transmitters will appear on any Quick Look display belonging to any Unit that has this option enabled.

NOTE: If the Check Band Warning Only, Escalate Check Band to Band Off Alarm, or Immediate Band Off Alarm settings are changed while alarms are active, these changes will be reflected immediately in the Configure Transmitter window (found on the Main tab of the Admit Information window) and may not represent the settings that were in force at the time the alarms were first displayed.

Wander Management

From the Wander Management section, the following options are available:

- **Enable Loiter notifications:** Click this checkbox on to control whether Loiter events will be created for Exit Alarm Controllers assigned to this Unit.

NOTE: Auto-Enrolled transmitters near doors in Units with Loiter notifications enabled will cause Loiter alarms to appear on all Clients.

- **Loiter Delay Time:** The number of seconds/ minutes that the system should wait before it initiates a loiter event. **The default delay is 5 minutes.**
- **Display Door Alarm at start of egress cycle**: Check this to create a Door Alarm when a Delayed Egress Exit Alarm Controller enters its egress mode. This provides advance notice that someone has been trying to open the door before it will open

and provides caregivers more time to react.

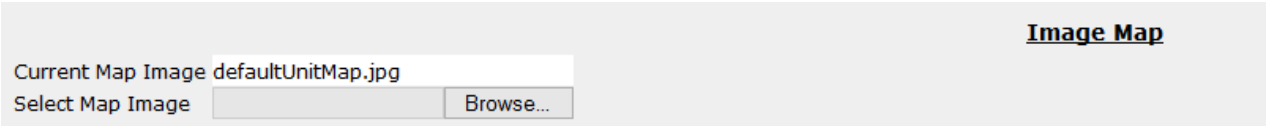


Image Map

From the Image Map section, the following options are available:

- **Current Map Image**
- **Select Map Image:** Click the **Browse...** button to search for the file.

NOTE: Maps can be in .jpg or .gif format. Maps created by the user must be made with light colors to reduce the appearance of fingerprints on touchscreen monitors.

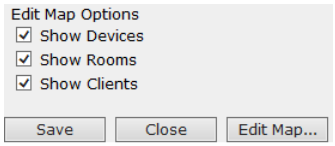
Device Selection

From the Device Selection, do the following steps:

- **Available Devices/Clients:** Select a device or devices you want to add to the unit.
- **Add >>:** Selected devices will appear in the **Assigned Devices/Clients** field when clicked
- **<< Remove**: If you want to remove a device from a unit, select the device(s) you want to remove from the Assigned Devices/Clients list and click Remove.

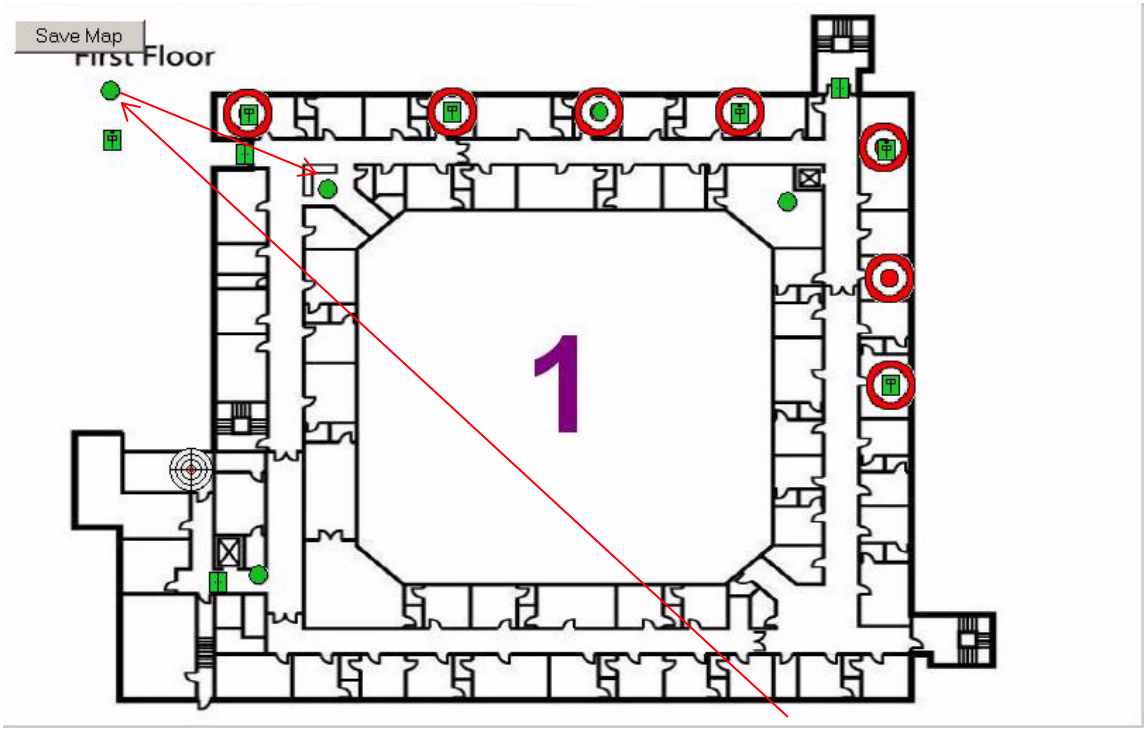
NOTE: Devices must not be assigned or unassigned from any unit if there are any active alarms in the system.

Edit Map Options



The Edit Map Options allow you to select to show the device, room and/or client icons on the Map Editor **(by default, all options are selected)**.

1. To position the devices in the correct areas on the map, click **Edit Map**
2. The **Map Editor** window opens.
3. Icons appear, one on top of the other, in the upper-left corner of Map Editor. Drag the icons to the appropriate locations on the map (see example on next page).
4. Click **Save Map** to save and return to the Unit Properties window.
5. When all Unit properties have been configured, click **Save** to save changes made.



Drag each icon to its location on the map or floor plan

WARNING: To avoid covering up active alarms, do not place device icons on top of each another, unless placing a device icon on top of the icon for the room that it is assigned

Viewing Unit Properties

To view unit properties:

1. Go to the **Configuration Rooms** window
2. Highlight the unit you wish to view and click **Properties…**
3. The **Unit Properties** window opens
4. If you change any properties of the unit, you must click **Save** to save your changes
5. If no changes were made, click **Close** to exit this window

Removing a Unit

To remove a unit:

1. Go to the **Configuration Rooms** window
2. Highlight the unit you wish to remove
3. Click **Remove**
4. A dialog box opens asking if you are sure you want to delete
5. Click **OK** to remove the room or **Cancel** to close the window without removing the room.

NOTE: You cannot remove a unit that has a patient assigned to it.

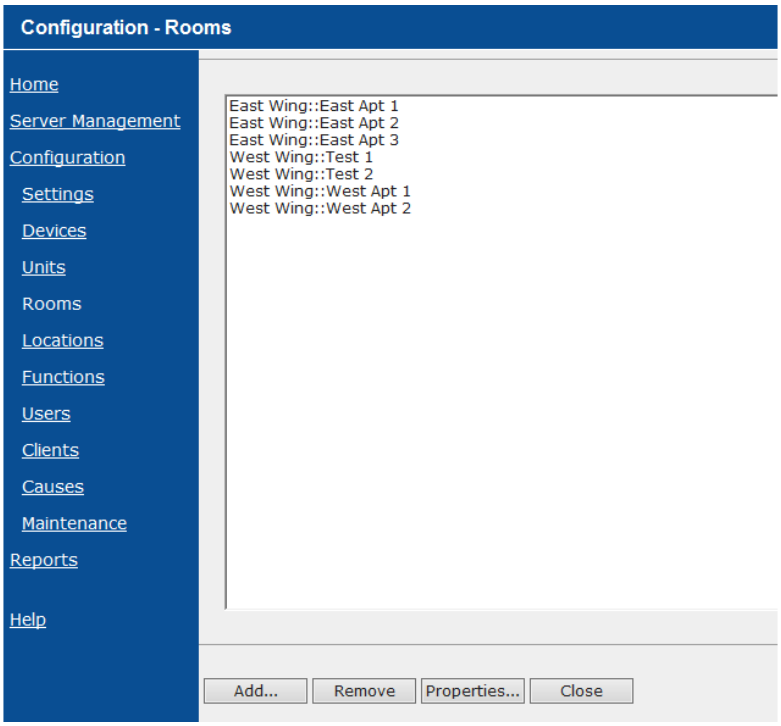
Configuring Rooms

The following section contains steps about adding and removing rooms to the system. In addition, it provides detailed information about viewing room properties.

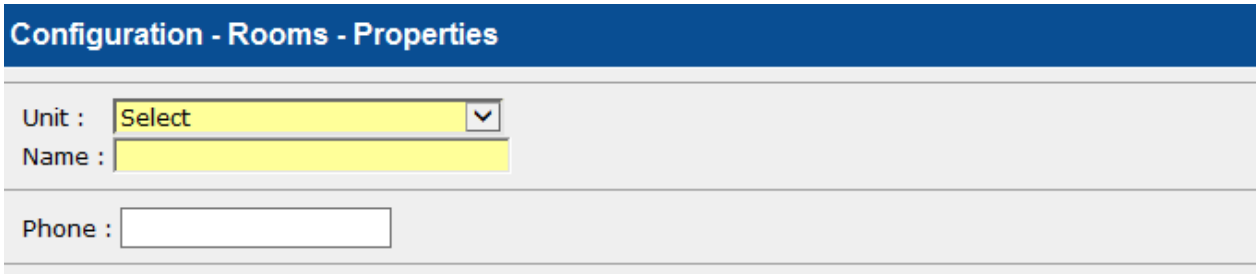
To configure a room:

1. Go to the **Configuration** home page
2. Select **Rooms**
3. The **Configuration Rooms** window opens

Adding a Room



4. Click **Add**
5. The **Configuration – Rooms – Properties** window opens



- **Unit**
- **Name:** Room names can only contain alphabetic and numeric characters, spaces, and the following special characters: **! - _ . ; [ ]{ }( )**
- **Phone:** Enter the PBX number or the number of the Cisco auto-answer phone. **NOTE**: When entering a PBX number, the PBX escape code should be entered followed by the room extension number, with no spaces (i.e. PBX1234).

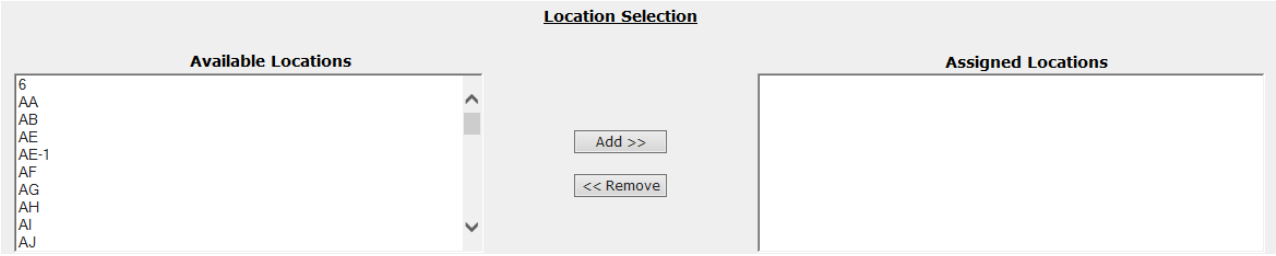
NOTE: The Unit and Room name field is limited on the Quick Look Display. The combined name length should not exceed 20 characters. The room number will be truncated should the combined characters exceed this limit. If this happens, the patient's room number will need to be verified in the Event Information window.

The Quick Look Display is a secondary means of alarm notification. For more specific patient or asset alarm information and location, reference the Client application.

Device Selection

From the Device Selection, do the following steps:

- **Available Devices:** Select a device or devices you want to add to the room.
- **Add >>:** Selected devices will appear in the **Assigned Devices** field when clicked
- **<< Remove**: If you want to remove a device from a room, select the device(s) you want to remove from the Assigned Devices list and click Remove.



Location Selection

NOTE: This option is only available if you are licensed for Quick Response Plus and Smart ID. Additionally, the Use Location Engine For Pendant Alarms checkbox has to be checked (refer to Global Settings).

From the Location Selection, do the following steps:

- **Available Locations:** Select a location or locations you want to add to the room. The locations are derived from a site survey conducted by RF Technologies.
- **Add >>:** Selected locations will appear in the **Assigned Locations** field when clicked

- **<< Remove**: If you want to remove a location from a room, select the location(s) you want to remove from the Assigned Locations list and click Remove.

NOTE: After saving changes to the Location Selection, you must reboot the Central Server to ensure that the changes have been implemented.

Adding a Room to the Map

To Place a room on the map:

1. Go to the **Configuration** home page
2. Select **Units**
3. Select the unit the room resides in and click **Properties...**
4. Click on **Edit Map**. The room icon will appear in the upper left corner of the map.
5. Click and drag the icon to the desired location
6. Click **Save Map** to save and return to the **Unit Properties** window
7. Click **Save** to save your changes

Viewing Room Properties

To view room Properties:

1. Go to the **Configuration Rooms** window
2. Highlight the room you wish to view and click **Properties**
3. The **Room Properties** window opens with options for you to add or remove devices to that room
4. If you change the properties of the room, you must click **Save** to save your changes
5. If no changes were made, click **Close** to exit this window

Removing a Room

To remove a room:

1. Go to the **Configuration Rooms** window
2. Highlight the room you wish to remove
3. Click **Remove**
4. A dialog box opens asking if you are sure you want to delete the room.
5. Click **OK** to remove the room or **Cancel** to close the window without removing the room.

NOTE: You cannot remove a room that has a patient assigned to it.

Chapter 2 – Software Configuration - System

Introduction

This chapter provides details on the System Management functions that were not covered in the Initial System Configuration chapter of this guide. This section follows the order that System Management links are displayed in the software. Functions in this section may be out of sequence from the normal order of configuration performed on the system.

System Management

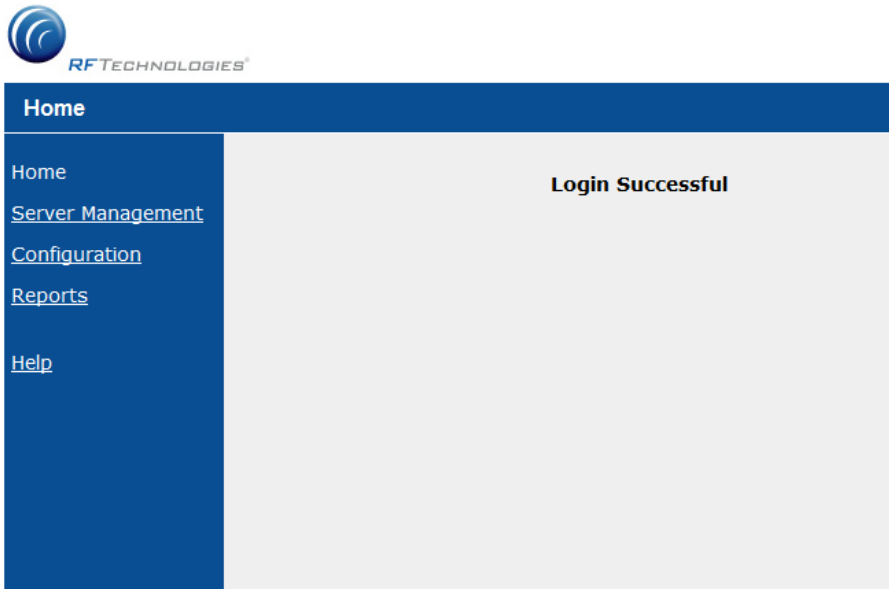
After the software is successfully installed on the Central Server and Client computer(s), the next step in the installation process is to define the System Configuration in System Management.

WARNING: The changes you make in System Management affect the entire system; you are not configuring just the Client computer, but all the Client computers at once. For instance, units are set up here and then each Client computer is configured to respond only to specified units.

The system only supports configuration changes from one computer at a time. If the Central Server and Client computer are both logged into System Management, changes made on one will not appear on the other until you exit and log back into System Management.

To access the System Management page:

1. Select **Login** select **Administrative Functions**
2. Select **Configuration**, or double-click the desktop icon if the Client application is not running
3. The System Management **Home** page opens

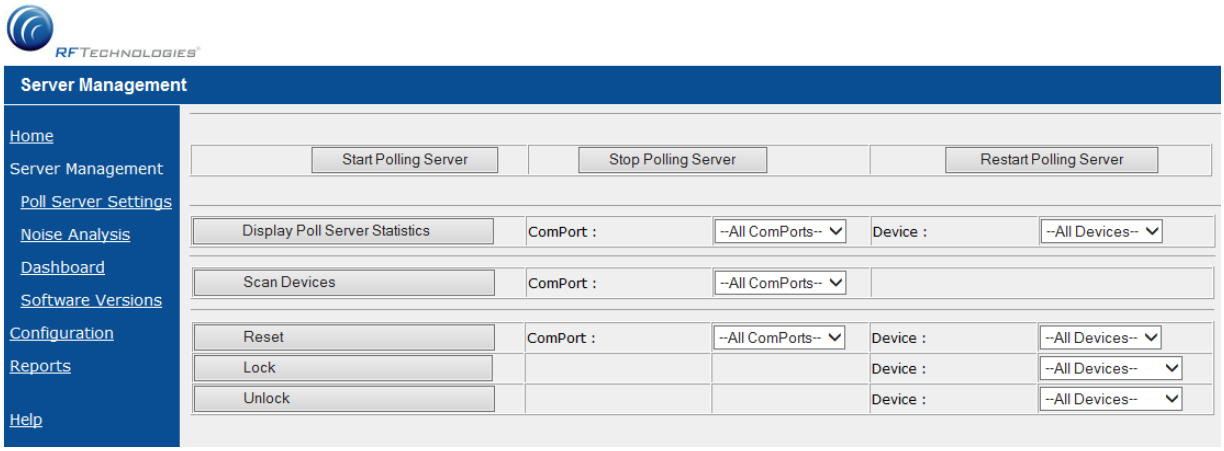


From the System Management home page, you can access the following:

- **Server Management**: Allows you to configure Poll Server Settings, view Noise Analysis and perform system diagnostics
- **Configuration:** Allows you to access menus to configure Settings, Units, Rooms, Devices, Users, Functions, Clients, Causes and Maintenance
- **Reports**: Allow administrators to create a report of archived data or unit details
- **Help:** Opens the on-line Users' Manual

Server Management

The Server Management window allows you to scan and reset devices, lock and unlock a global lockdown, along with configure Poll Server Settings, Noise Analysis, view the Dashboard, and view the list of installed RFT Software files.



To access the Server Management page:

1. **Login** then select **Administrative Functions**
2. Select **Configuration**, or double-click the desktop icon if the Client application is not running
3. Select **Server Management**

Polling Server

The Polling Server application can be stopped, started, or restarted from the Server Management window. Additionally, you can display the Poll Server Statistics, reset devices, and lock/unlock door controllers for global lockdown.

Start / Stop / Restart Polling Server

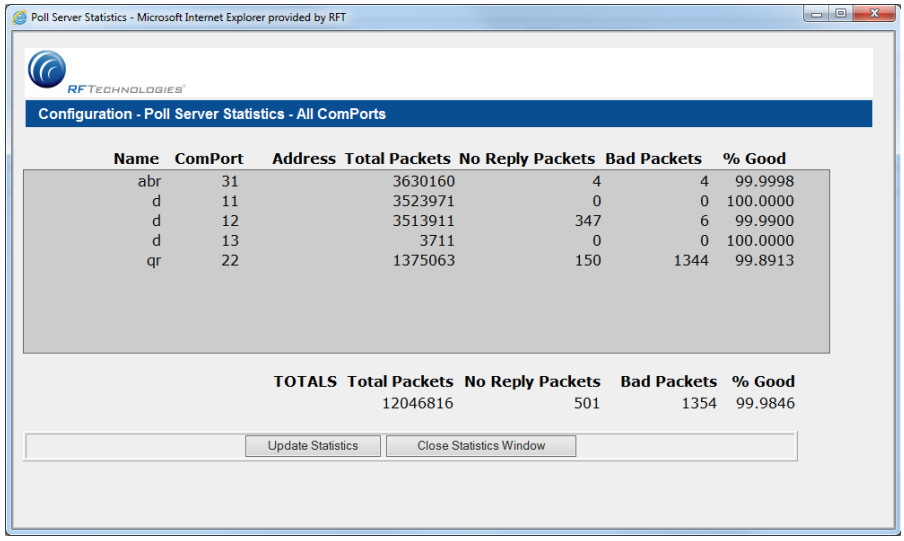
To start / stop / restart the Polling Server:

1. Go to the **Server Management** home page
2. Click **Start Polling Server** to start the Polling Server application
3. Click **Stop Polling Server** to stop the Polling Server application
4. Click **Restart Polling Server** to restart the Polling Server application

Display Poll Server Statistics

To display Poll Server Statistics:

1. Select **All ComPorts** (or individual)
2. Select **All Devices** (or individual)
3. Click **Display Poll Server Statistics**
4. The Polling Server Statistics window opens with information on the polling for all Com Ports



Reset

If a 9450 System device or Quick Reference Premiere Wireless Call System hardware device (Gateway and Router) is not functioning correctly, you can use the software to reset it.

To reset devices:

1. Go to the **Server Management** home page
2. Select **All ComPorts** (or individual) from the ComPort pull-down
3. Select **All Devices** (or individual) from the Device pull-down
4. Click **Reset**. A Reset Successful dialog box appears to confirm that the reset was successful

NOTE: Only perform this process if a Device Fault alarm occurs and has been properly handled per your facility's policy. This process is also used to zero out the polling service polling statistics.

Lock / Unlock

The lock/unlock features allow you to lock or unlock one specific or all 9450 Door Controllers configured for global lockdown.

To lock and unlock doors:

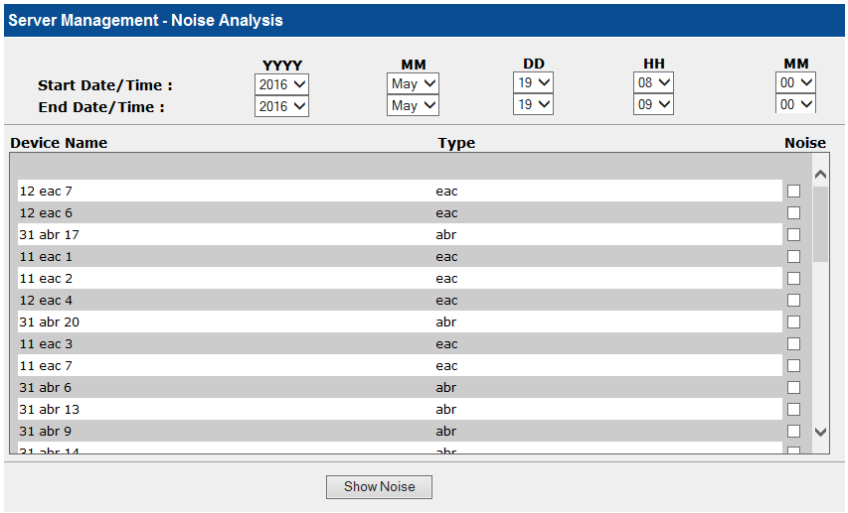
1. Go to the **Server Management** home page
2. Select **All Devices** (or individual)
3. Click **Lock** to lock all 9450 Door Controllers configured for global lockdown
4. Click **Unlock** to unlock all 9450 Door Controllers configured for global lockdown

Noise Analysis

From the Noise Analysis window you can search for RF noise affecting 9450 devices in the system.

To run a Noise Analysis:

1. Go to the **Server Management** home page
2. Select **Noise Analysis**
3. The **Configuration - Noise Analysis** window opens



4. Select the **Start Date/Time** and the **End Date/Time** for the analysis
5. Select the **Device Name** (a maximum of 4 devices can be selected)
6. Click **Show Noise**
7. A noise analysis report of the selected device opens. If no noise data was found, you will be prompted to select another device

Dashboard

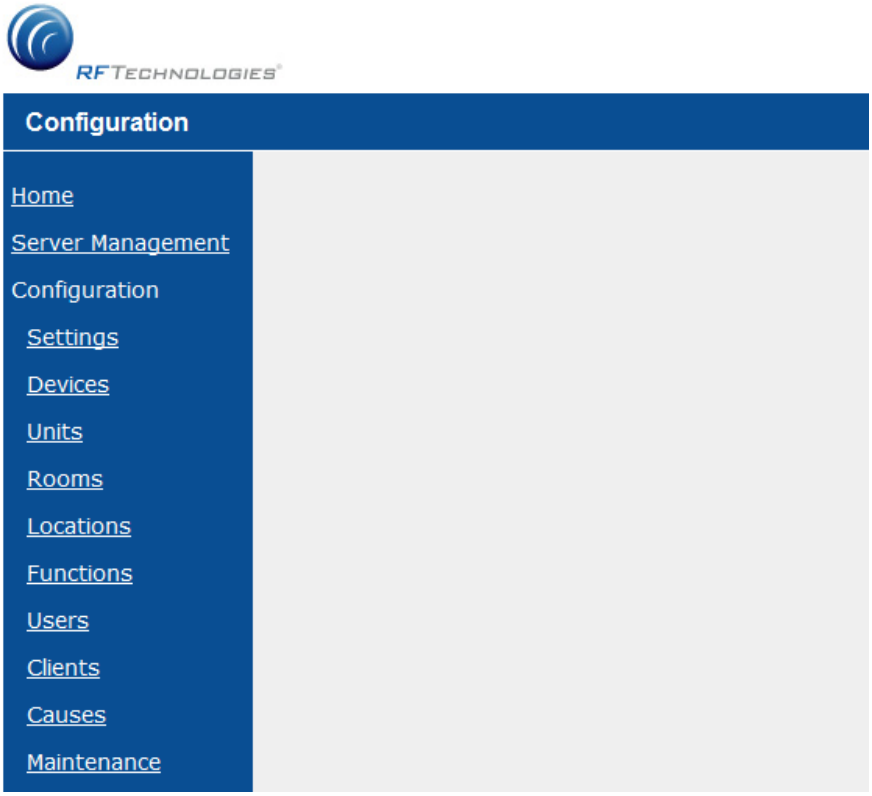
The Dashboard shows you a static picture (snapshot) taken every 5 seconds of the real-time data of the system, including Devices, Transmitters, Clients, and Events, along with information on Quick Response Plus Supervision Information and Transmitter RSSI data. For more information about the Dashboard, contact the Technical Support Team at (800) 669-9946 or (262) 790-1771.

Software Versions

The Software Version window shows a listing of all RFT files loaded on the server, along with their size and last modified date for troubleshooting purposes only.

Configuration

The Configuration option allows you to add and configure devices, units, rooms, users, and alarm causes. You can also update location names, password protect system functions, create alias names for client computers, and maintain configuration information along with people and assets.



To access the Configuration Home page:

1. **Login** then select **Administrative Functions**
2. Select **Configuration**, or double-click the desktop icon if the Client application is not running
3. Select **Configuration**

Settings

When all devices are added to the software database and units are defined, confirm that all of the system-wide settings are set according to the standards of your facility.

From the Configuration page, click on Settings to display links to configure these settings:

- Global
- Transmitter ID Ranges
- Quick Response Plus Device ID List
- Card Reader Strings
- Messaging
- Pager Hardware
- CISCO Settings
- Walkie-talkie

Global

Global Settings allow you to enter the facility's demographic information, enable General and 9450 features such as dialog message prompts, enable and configure Lockdown settings, and enable the Auto-Enroll transmitter feature.

Following are details on configuring each Global Setting. Once all settings are configured, select **Save** to save the settings and close the window. Selecting **Close** will close the window but will not save your settings.

NOTE: Your actual screen may be different depending on your license

To access the Global Settings:

1. Go to the **Configuration Home** page
2. Select **Settings**
3. Select **Global**
4. The **Configuration – Settings – Global** window opens

Facility

The Facility portion of the Global Settings window allows you to enter your facility's Report Header information. This information is printed on all reports generated by the system.

Enter the information as it should appear in your reports

NOTE: Once facility information is entered, you must reboot the system before Report Header information is displayed on reports generated by the system.

General

The General portion of the Global Settings window allows you to enable general features such as dialog message prompts and what is displayed on the Quick Look display. Following are detailed descriptions of the options under General settings. Click the checkbox if you wish to enable the setting.

- **HIPAA Options**:
  - No HIPAA Filtering—When selected, the resident/patient first and last name will display **(default for Code Alert)**.

- HIPAA (Do Not Show First Name)—When selected, only the last name will display.
- HIPAA (Show Room Number Only)—When selected, only the Room Number will display **(default for Safe Place)**.

NOTE: Due to the change to HIPAA Options, it is necessary to re-configure the HIPAA settings if you are upgrading from a version prior to the Series 9.4 Software.

Patient Information entered during Admit	What is displayed on the Quick Look Display
First and Last name	Last name, First name
Last name only	Last name
First name only	First name
If HIPAA Option is set to Do Not Show First Name	Last name-Gender
If HIPAA Option is set to Show Room Number Only	Room-Gender

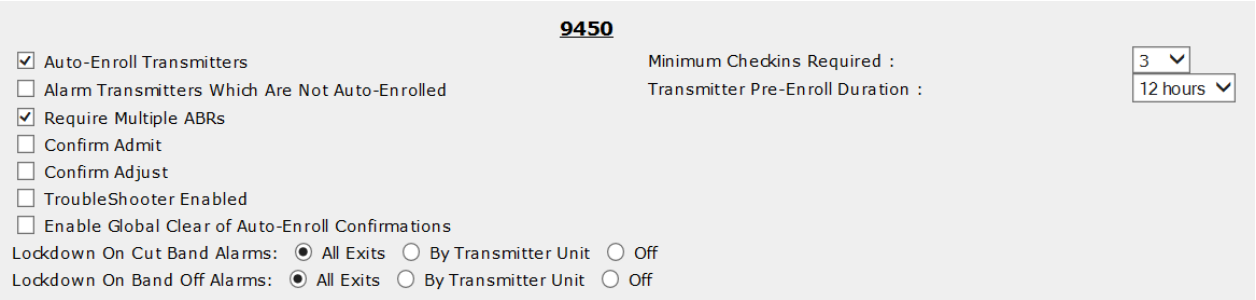
- **Show Date and Time on Quick Look:** Show the date and time on the Quick Look display when there are no alarms. **By default, this option is selected.**
- **Hide Workstation Map Device Icons:** Hides the device icons on the workstation's Map view.
- **Confirm Discharge:** When enabled, a dialog box appears after the Discharge is complete to confirm that the Discharge was successful.
- **Confirm Escort or Transfer:** When enabled, a dialog box appears after the Escort or Transfer is complete to confirm that it was successful.
- **UL-1069 / UL-2560 Low Battery Alarm Notification:** When checked, Low Battery alarms will appear as Yellow Device Fault alarms in the Client Software.
- **Hide Event Times in Client Lists: (Code Alert only)** When checked, the event time will not be shown in the client's Event List view, nor in the list of active events in the Census and Map views. In Safe Place, the setting is hidden and unchecked.
- **Alarm Volume Level**: Allows you to select from the drop-down the alarm volume level of the Client application. The range is from **100% (default)** down to 10% of the volume as set by the computer's operating system in decibels (dB).
- **Alarm Silence Timeout After**: Allows you to select from the drop-down the time (in seconds) when an Alarm Silence will expire–1 to 10 minutes **(default 5)**. The Silence button enables you to silence an alarm only at the computer where the Silence button is pushed.
- **Auto Close Software**: The Client software will automatically close after so many minutes of a user's inactivity. This option

allows the user to set the minutes of inactivity before software closure, **1 (default)** to 60 minutes. Mouse or key activity on the Client will reset the inactivity countdown timer back to zero

NOTE: The functionality to enable the Auto Close Software feature is found in the Client Properties window for the individual computers. The feature is disabled by default. For Clients running on the same computer as the Server, the Auto Close Software feature is not configurable.

WARNING: Caution must be taken when enabling this feature as alarms will not be sent to the Client once its application is closed. You must restart the Client application when you enable or disable the Auto Close Software feature for the change to occur.

- **Inactive User Log Off**: The Client software will automatically log off the user and return to the Main View after so many minutes of inactivity. This option allows the user to set the minutes of inactivity before logoff, **1 (default)** to 60 minutes. Mouse or key activity on the Client will reset the inactivity countdown timer back to zero.
- **Timed Event Warning Time**: Allows you to select from the drop-down the time before the expiration of an event, that a Timed Event Warning is issued–1 to 60 minutes **(default 5)**. Examples of Timed Event Warnings are Escort to Expire and Transfer to Expire.
- **Workstation Default Screen**: Use this option to set the default screen you want displayed on the workstation when an alarm occurs. Choose between Map, **Census (default)** or Event List.
- **Device Fault / Low Battery Alarm Silence Period**: This is the length of time that device fault and low battery alarms will remain silent when the Silence button is clicked. This is configurable for 1 hour, 4 hours, and **24 hours (default)**.
- **Workstation Census View Column Order**: Use the pull-downs to select the order census information is displayed on the workstation.



9450 The 9450 portion of the Global Settings window allows you to enable 9450 features such as confirming Admit and Adjust and confirming that all of the Auto-Enroll settings are set according to the standards of your facility. Click the checkbox if you wish to enable a setting.

If the Auto-Enroll feature is enabled, transmitters can be automatically

detected and enrolled into the system. If the Lockdown feature is enabled, exits equipped with CodeLock™ electromagnetic locks and elevators using Elevator Deactivation can be configured to lock/deactivate in the event of a Cut Band or Band Off Alarm

NOTE: For 9450 systems, there is an increased device fault delay following startup. The system will wait 3 minutes after the server computer and polling has started before posting any device faults from the 9450 equipment. This delay will prevent the posting of erroneous faults while the system is coming online.

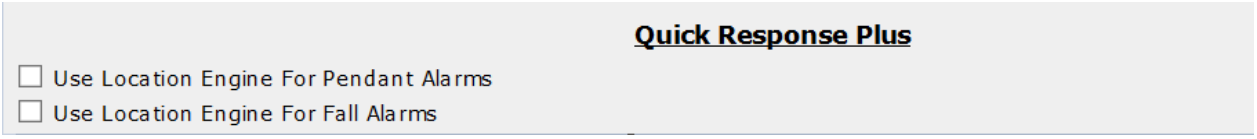
- **Auto-Enroll transmitters:** Turns on the Auto-Enroll function. **By default, this option is selected.**
- **Alarm Transmitters Which Are Not Auto-Enrolled**: Display Cut Band Alarms for all transmitters, enrolled or not, that are within the configured ID range.
- **Require Multiple ABRs**: Requires more than one Alarming Band Receiver to receive a check-in from the transmitter before the system Auto-Enrolls it.
- **Confirm Admit or Adjust**: When enabled, a low priority white alarm appears after the Admit or Adjust has completed to confirm that it was successful. **By default, this option is selected.**
- **Require Mother/Infant Match Before Discharge**: When enabled, a Match alarm is issued if an infant is discharged and the banding material on the infant transmitter is cut before performing a Mother/Infant match.
- **Troubleshooter Enabled**: When enabled, a Troubleshooter dialog box appears after three consecutive No Signal alarms are received and you have clicked in the Alarm Message Box of the third alarm. The Troubleshooter dialog box prompts the user to close the dialog, discharge the tag, and choose whether the tag is in use or not. Closing the Troubleshooter opens the Event Information window for clearing the alarm.
- **Enable Global Clear of Auto-Enroll Confirmations:** When enabled, auto-enroll confirmation messages on client PC's may be cleared by the user and the confirmations will be removed from all client PC's. When disabled, the confirmation messages can only be removed by:
  - Naming the auto-enrolled transmitter
  - Adding the transmitter as an asset
  - Marking the transmitter as missing
  - Discharging the auto-enrolled transmitter
- **Lockdown On Cut Band Alarms**: When Lockdown on Cut Band alarm is selected, the lockdown feature is activated; if a Cut Band alarm is issued, the exits specified are automatically locked. Options for the Lockdown feature are as follows:
  - **All Exits**: When selected and a Cut Band alarm is issued, all exits equipped with CodeLock electromagnetic locks will lock and elevators using Elevator Deactivation will deactivate. **This is the default selection.**

- **By Transmitter Unit**: When selected and a Cut Band alarm is issued, only the exits associated with the transmitter's specified unit will lock. If a transmitter issues a Cut Band alarm and it is not in the area defined by the unit, it will not be protected by the lockdown feature. If your facility is using the Lockdown by transmitter unit, you are advised to assign each Exit Alarm Control Unit equipped with CodeLock™ electromagnetic lock to only one unit.
- **Off**: When selected, the lockdown feature is turned off.

- **Lockdown On Band Off Alarms**: When Lockdown On Band Off Alarms is selected, the lockdown feature is activated; if a Band Off alarm is issued, the exits specified are automatically locked.

WARNING: When you select Lock down by Transmitter Unit, if a Cut Band or Band Off alarm occurs while the patient is in Transfer or Escort, and the patient has left the unit, the system will default to Global Lockdown all exits.

- **Minimum Checkins Required:** The minimum amount of check-ins required before the system Auto-Enrolls a transmitter **(default is 3)**.
- **Transmitter Pre-Enroll Duration: (Available for Safe Place only)** Use the pull-down to select how long a transmitter can be "reserved" prior to enrollment (used during the pre-admission/pre-enrollment process). **Default is 12 hours.**



Quick Response Plus

The Quick Response Plus setting allows the user to Disable/Enable using the Location Service to report a detailed location for Quick Response Plus Pendants or Sensatec devices, if a location database has been installed. **(Available for Code Alert only)**

- Check the **Use Location Engine For Pendant Alarms** checkbox to enable the setting, un-check the checkbox to disable the setting.
- Check the **Use Location Engine For Fall Alarms** checkbox to enable the setting for Sensatec devices, un-check the checkbox to disable the setting.

Authentication

LDAP authentication verifies whether a user has a valid ID and password and that they are enabled within the system. It uses your existing Active Directory password policies (strength, expiration policy, etc…) and allows for disabling accounts after so many failed logins to strengthen your system security.

This option requires an RFT LDAP license and a configured server on your network.

NOTE: After any of the LDAP settings are changed, the RFT server must be rebooted in order for the new settings to take effect.

CAUTION: The Active Directory passwords **cannot** contain the following special character: **+**.

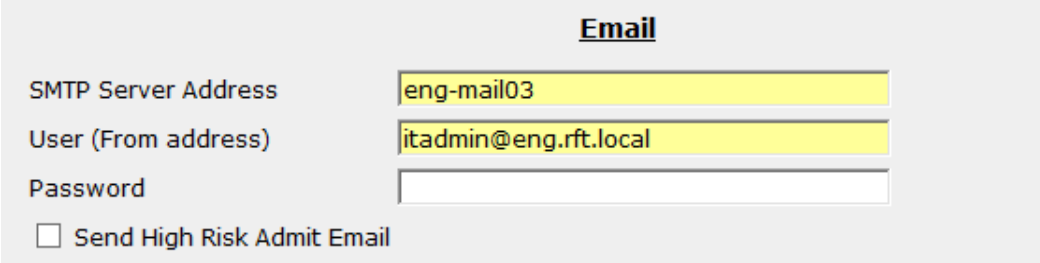
- **Enable LDAP Authentication**: Check this box to send login requests to an LDAP server instead of using the internal user database.
- **LDAP Server Hostname**: The hostname or IP address of the facility's LDAP server.
- **Domain Name**: Only one domain is supported. The domain can be found in the Windows logins as user@domain, or domain/user.
- **Authentication Cache Expiry**: Once a user logs in successfully, the successful login can be re-used with the correct credentials for a limited period of time. This reduces the number of login requests sent to the LDAP server. If all login requests should be sent to the LDAP server, set this value to 0 seconds.
- **Login Requires**: Two methods of login are supported with LDAP, manual entry and two-factor authentication.
  - **Card & Password Only** (formerly Two-Factor Authentication): A swipe/proximity card is used to identify the user and then the user must also enter their password. All clients must have the correct type of card reader installed.
  - **Card/Login & Password**: The username is either typed manually, or using a swipe/proximity card. The password is manually typed into the login dialog.

NOTE: User accounts with "dummy" passwords should be setup **prior** to enabling this feature (see *Adding a User* for additional details). Once LDAP authentication is enabled, the users login to the software using their windows credentials and the "dummy" password is wiped out.

- **Port Number:** Default value is 389
- **Maximum Invalid Logins**: If a user enters an incorrect password to log into either a client or configuration this many times, their account is disabled in Safe Place/Code Alert.
  - If a user account is disabled, it must be re-enabled on both the LDAP server and within the RFT server's configuration screen (**Disabled Users Information** page).
- **Bind Method**: This is fixed to Negotiate.

- **Enable Kerberos**

NOTE: When disabling a user account, the account must be disabled on both the LDAP server and within the RFT server to prevent unauthorized access.



Email The Email settings allow the user to configure the email server.

NOTE: This option is only available if your system is licensed for SMS/SMTP.

- **SMTP Server Address:** Enter the address to be used for email transfers.
- **User (From address):** The first part of the address, up to the "at" sign (@), will be used to log into the mail server.
- **Password**
- **Send High Risk Admit Email: (Available for Safe Place only)** Click the checkbox if you wish to enable the feature **(default is unchecked)**. Admitting an Asset as High Risk also results in a High Risk email being sent.

Escort Destinations The Escort feature allows the user to select a destination to which the patient is to be escorted. Pre-determined destinations can be set up from the Escort Destination section. This setting also allows you to **Enable Mom-Baby Time Tracking for Escort Destinations (Safe Place only)**. When enabled, the Escort event is documented in the Mom-Baby Time Tracking Detail Report as time spent away from mother **(default is unchecked)**.

To add a Destination:

1. Place the cursor in the **Add** field and type in a destination.
2. Click **Save**. The Description list populates with the new destination.
3. The list displays the top three destinations in the order they were entered. Use the scroll bar to view the complete list of destinations.
4. Click **Close** to return to the main Settings window.

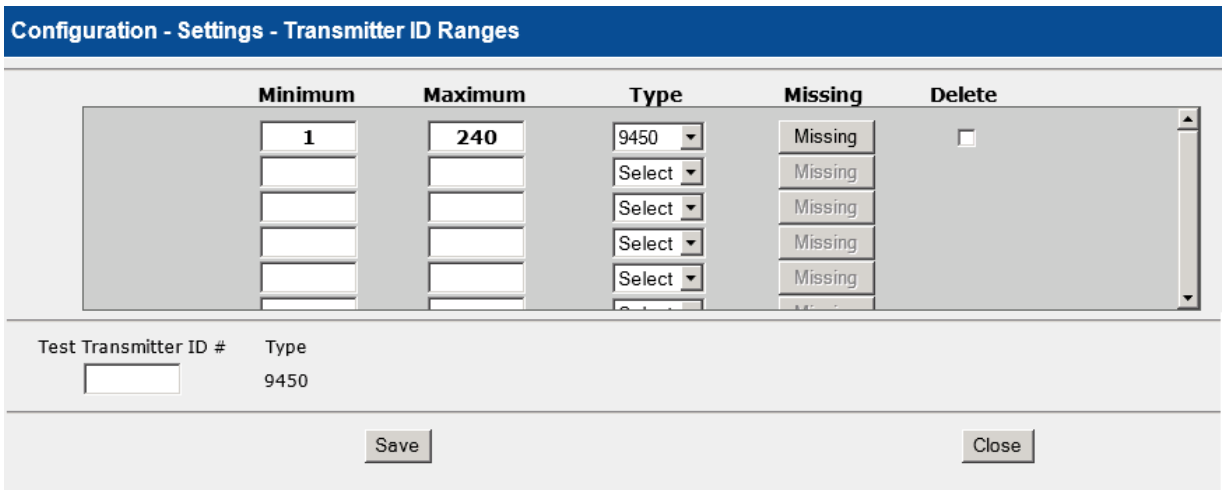
To remove the Destination:

1. Click the **Remove** checkbox next to the destination you wish to remove
2. Click **Save** and the Description list refreshes with your changes
3. Click **Close** to return to the main Settings window

Transmitter ID Ranges

The Series 10.x Software supports various ranges of Transmitter ID numbers. The ranges of Transmitter ID numbers are configured in the software to prevent a group of Transmitter ID numbers from another facility's system from setting off alarms in your system.

NOTE: The Transmitter ID Ranges feature is only used for 9450 transmitters.



To add a Transmitter ID Range:

1. Go to the **Configuration** home page
2. Select **Settings**
3. Select **Transmitter ID Ranges**
4. The **Configuration – Settings – Transmitter ID Ranges** window opens
5. Enter the minimum and maximum IDs to be used for the facility's transmitters
6. Select the transmitter **Type** from the pull-down
7. Click **Save** and the screen refreshes with your changes

To delete a Transmitter ID Range:

1. Go to the **Transmitter ID Ranges** window
2. Click the **Delete** checkbox next to the range of transmitters you wish to delete
3. A dialog box opens asking if you are sure you want to delete this range, click **Ok** to confirm
4. Click **Save** to delete the transmitter range and the screen refreshes with your changes

NOTE: If you are narrowing the Transmitter ID Range so that you do not have missing transmitters outside the ranges, simply delete the range and enter new minimum/ maximum ranges.

To delete a Transmitter ID Range that contains a Quick Response device:

1. Remove the device from the room
2. Remove the device from the unit
3. Delete it from the **Device List**
4. Delete the **Transmitter ID Range**

WARNING: When deleting a range of transmitters (for example, 1 through 9), verify that no patient is assigned to a transmitter within that range. For example, if a patient is assigned to transmitter 7, the system will allow for transmitter 7 to be deleted if it falls within the deleted range.

Missing Transmitters

To remove Missing Transmitters from an ID Range:

When a No Signal alarm occurs for a transmitter number that does not exist in your system or that has not been activated, you can remove that transmitter number from the Transmitter ID range.

1. Go to the **Transmitter ID Ranges** window
2. Select the **Missing** button next to the range that corresponds to the missing transmitter number
3. Enter the missing transmitter number
4. Click **Save** then click Close to return to the main window

To remove a Transmitter from Missing:

1. Go to the **Transmitter ID Ranges** window
2. Select the **Missing** button next to the range that corresponds to the missing transmitter number
3. Click the **Remove from Missing** checkbox next to the missing transmitter number
4. Click **Save** and the screen refreshes with your changes
5. Click **Close** to return to the main window

Test Transmitters

To designate a transmitter as a Test Transmitter:

A transmitter can be designated as a test transmitter. When a test transmitter goes into alarm, the alarm is silent at the Client computer and at the Quick Look display. All other alarm functions are applicable.

1. Go to the **Transmitter ID Ranges** window
2. In the **Test Transmitter ID#** field, enter a transmitter ID number for a 9450 transmitter that is from one of the configured ranges
3. Click **Save**
4. Click **Close** to return to the main Settings window

Repeater/Locator Ranges

Additional Repeaters and Locators can be added by extending the normally allowed ID range. The minimum and maximum normally allowed ID range for Repeaters and Locators are shown in the following table.

	Min	Max
Repeaters	65281	65405
Locators	65406	65535

To extend a Repeater or Locator Range:

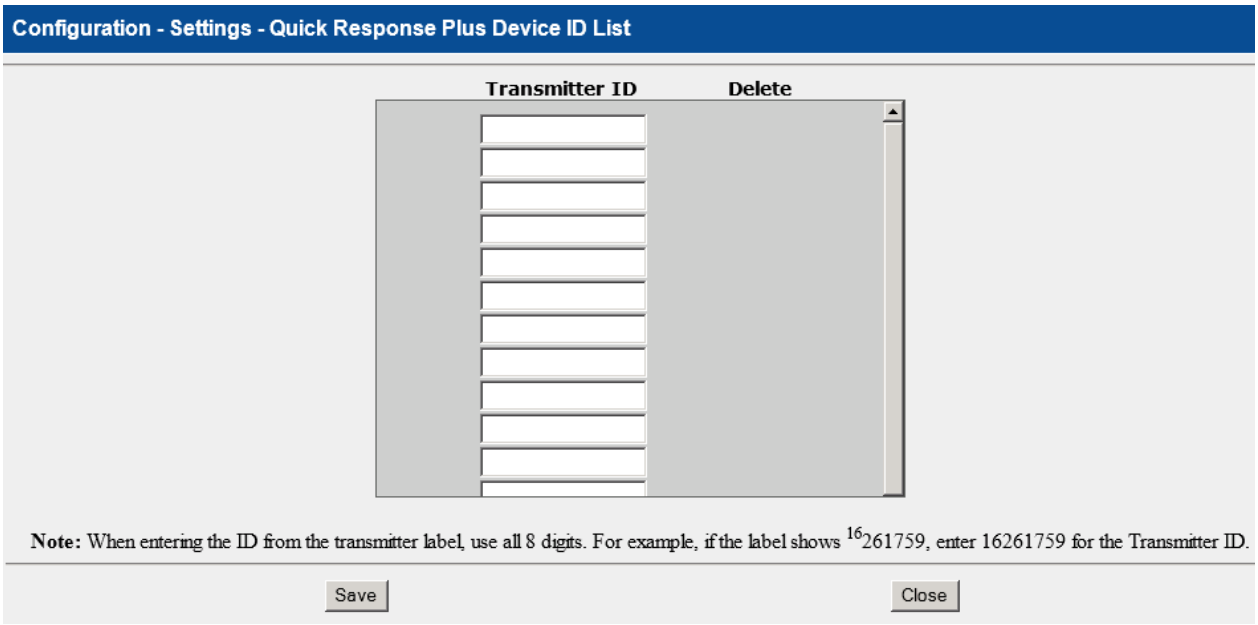
1. You must first enter the range to display a list of Transmitter ID Ranges
2. Place the cursor in the empty field and type in a **Minimum** ID number and a **Maximum** ID number. You can enter a single ID number (same ID number entered for Min and Max) or you can enter a range of ID numbers
3. From the **Type** pull-down, select the type of device (Repeater or Locator)
4. Click **Save** and the list populates with the new range
5. Click **Close** to return to the main Settings window

To remove a Repeater or Locator Range:

1. You must first enter the range to display a list of Transmitter ID Ranges
2. Click the **Delete** checkbox next to the range you wish to remove
3. Click **Save** and the list refreshes with your changes
4. Click **Close** to return to the main Settings window

Quick Response Plus Device ID List

The Quick Response Plus Device ID List allows you to add Quick Response Plus devices into the system. Devices are added by entering the transmitter ID number in the Transmitter ID field. The transmitter number can be found on the device's enclosure as well as the circuit board.

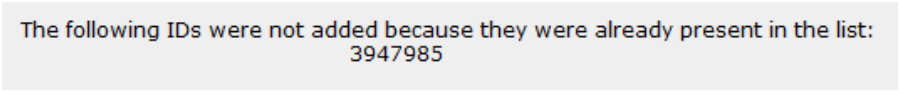


To access the Quick Response Plus Device ID List:

1. Go to the **Configuration** home page
2. Select **Settings**
3. Select **Quick Response Plus Device ID List**
4. Click in a blank **Transmitter ID** field

NOTE: Initially there are 32 blank fields to use when adding Quick Response Plus devices to the system. After adding Transmitter IDs to the list and clicking **Save**, another 32 blank fields will be provided.

5. You must enter **all** 8 numbers for the transmitter. The allowed range for a transmitter ID is (1 through 16,777,215). An attempt to enter a transmitter ID outside of the allowed range results in an error message *"One or more IDs are out of the acceptable range (1 thru 16777215)"*
6. If a duplicate ID is entered, a message will display at the bottom of the Quick Response Plus Device ID List



7. Click **Save** to add the transmitter ID to the active range. The screen refreshes with your changes.

To delete a Transmitter ID:

1. Open the **Quick Response Plus Device ID List**
2. Click the **Delete** checkbox next to the transmitter ID you wish to delete
3. A dialog appears asking you if you are sure you wish to delete the transmitter ID from the system
4. Click **OK** to confirm the deletion

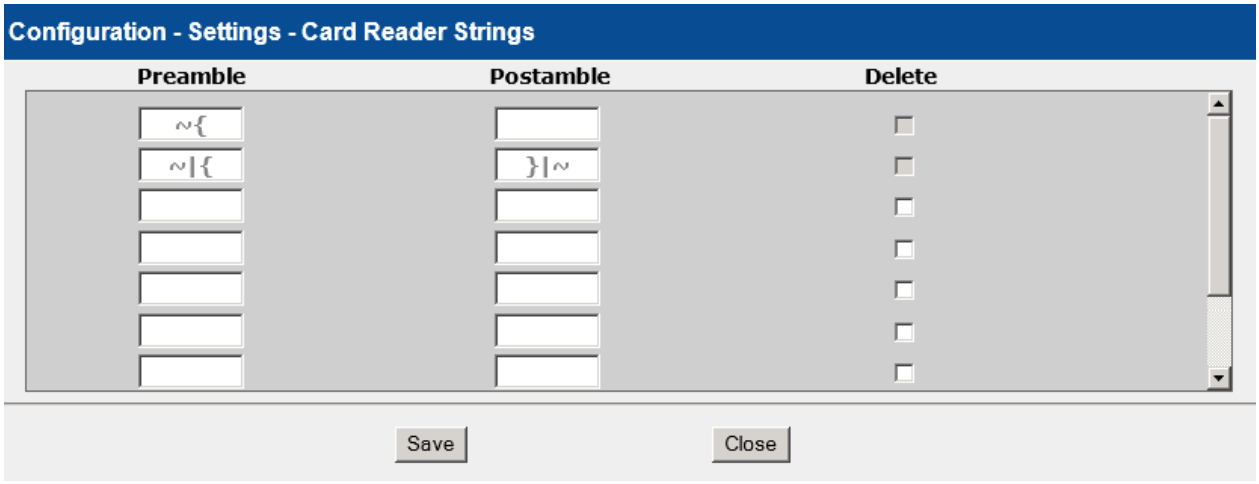
5. Once the transmitter IDs to be deleted have been selected, click **Save** to save your changes and remove the IDs from the list

WARNING: Any device or transmitter with the Delete checkbox checked on will be removed from the system. Its association with any room, unit, and/or patient will be removed as well.

Card Reader Strings

The card reader is a feature that allows a user to access the software by swiping a card with an identifying bar code or magnetic strip. If your facility is using the card reader feature, connect the card reader device to the Central Server and/or Clients and enable the feature in the software.

NOTE: Ensure the CAPS lock is not enabled on the computer while assigning a user. When assigning a card reader to a user, if the CAPS lock key is enabled on the computer, then the CAPS lock key must be on every time the user logs in. Otherwise, an invalid login attempt is recorded.



Test a USB Card Reader device to ensure proper operation:

1. Plug the card reader into an available USB port in the computer
2. The card reader beeps once and the red light on the device illuminates, indicating that power has been provided

Preamble / Postamble

The Preamble is a string of characters (key code) inserted at the beginning of the barcode data string. The Postamble is a string of characters appended to the end of the barcode data string. You may enter any special characters to prompt the software to start and stop reading the card reader's data string.

How to identify Preamble and Postamble text strings:

1. Open the Microsoft Windows Notepad application
2. Use identification card

3. Use the beginning and ending character sets for the preamble and postamble settings

To enter the Preamble and Postamble:

1. Go to the **Configuration** home page
2. Select **Settings**
3. Select **Card Reader Strings**
4. In the **Preamble** field, enter any special characters to prompt the software to start reading the card reader's data string
5. In the **Postamble** field, enter any special characters to prompt the software to stop reading the card reader's data string
6. Click **Save** and the screen refreshes with your changes
7. Click **Close** to return to the main Settings window

To delete the Card Reader settings:

1. Go to the **Configuration** home page
2. Select **Settings**
3. Select **Card Reader Strings**
4. Click the **Delete** checkbox next to the string to be deleted
5. Click **Save** and the screen refreshes with your changes
6. Click **Close** to return to the main Settings window

Messaging

The software contains messaging functionality that enables the system to message system events and information to the facility staff via the standard pagers, email, Cisco phones, smartphones, or text messaging. This section provides detailed information about messaging with the software.

NOTE: White Alarms that are configured at the Client level (i.e. Auto-enroll) cannot be messaged to Cisco phones (or smartphones).

To access the Messaging settings:

1. Go to the **Configuration** home page
2. Select **Settings**
3. Select **Messaging**
4. The Messaging home page opens with available links to allow you to configure Messaging settings for:
   - Devices
   - Groups
   - Units

Devices

The Devices menu allows you to add recipients for Pager, Email, Text, Phone and Smart Phone. Additionally you can Remove, Edit and view Messaging Properties.

To access the Devices window:

1. From the **Messaging** page, click the **Devices** link
2. The **Configuration - Settings - Messaging - Devices** window opens

To add a recipient for Paging:

1. From the **Configuration - Settings - Messaging - Devices** window click **Add Pager…**
2. Type the **Name** of the staff member to whom the pager is assigned
3. In the **Number** field, type the pager's ID number
4. Type a **Description** of the pager
5. Click **Save**
6. The Pager you added appears in the Devices list with Pager next to his/her name

To add a recipient for Email:

NOTE: To add an email recipient, the recipient must be set up as a User with an email address entered in the system.

1. From the **Configuration - Settings - Messaging - Devices** window click **Add Email…**
2. Select email recipient from the **User** pull-down. The Email Address automatically populates for that user.
3. Type any necessary **Description** of the email recipient
4. Click **Save**
5. The recipient you added appears in the Devices list with Email next to his/her name.

To add a recipient for Text messaging:

NOTE: To add a text message recipient, the recipient must be set up as a User with a text address to receive messages entered in the system.

1. From the **Configuration - Settings - Messaging - Devices** window click **Add Text….**
2. Select the text message recipient from the **User** pull-down. The Text Address for the recipient automatically populates for that user
3. Type any necessary **Description**
4. Click **Save**
5. The recipient you added appears in the Devices list with Text next to his/her name

To add a recipient for Phone messaging:

NOTE: You must verify that the Cisco phone is not assigned to a user before modifying its configuration. Changing the configuration of a Cisco phone while it is assigned to a user will un-assign it from that user.

Cisco phones require a unique extension for each phone configured to receive messages. Anomalies will occur when multiple Cisco phones (for example, desk phone and mobile phone) are configured with the same extension.

1. From the **Configuration - Settings - Messaging - Devices** window click **Add Phone…**
2. Type a **Name** used to identify the phone
3. Type the **Phone Number** or extension with no dashes
4. Type any necessary **Description**
5. Click **Save**
6. The phone you added appears in the Devices list with Phone next to his/her name

To add a recipient for Smartphone messaging:

DISCLAIMER: The RFT Cares Smartphone app is dependent on your site's Wi-Fi infrastructure for the reliable delivery of alarm notifications. If this application is the primary or most typical means of alert communication, it is critical that your site have robust Wi-Fi coverage and a well-managed Wi-Fi infrastructure. Customers are ultimately responsible for ensuring and maintaining reliable 802.11b, 802.11g or higher coverage with a minimum RSSI of at least -70dBm in all areas where the RFT Cares mobile devices are utilized.

Administration of the Wi-Fi network infrastructure, network traffic routing, firewalls, and network congestion monitoring is the sole responsibility of site IT staff or service providers.

1. From the **Configuration - Settings - Messaging - Devices** window click **Add smartphone…**
2. Type the **Name** of the staff member to whom the Smartphone is assigned

3. In the **Smartphone MAC** field, type the Smartphone's MAC address (obtained from the RFT Cares App or the Smartphone Settings)

NOTE: The RFT Smartphone Web Server relies upon the phone's MAC address, since the IP address the wireless network assigns to any given Smartphone may vary. In other words, the MAC address is assumed to be an invariant (never changing) that can be relied upon to uniquely identify each Smartphone device, regardless of how the wireless network assigns IP addresses.

4. Type a **Description** of the Smartphone
5. Click **Save**
6. The Smartphone you added appears in the Devices list with Smartphone next to his/her name

To edit a Messaging Recipient:

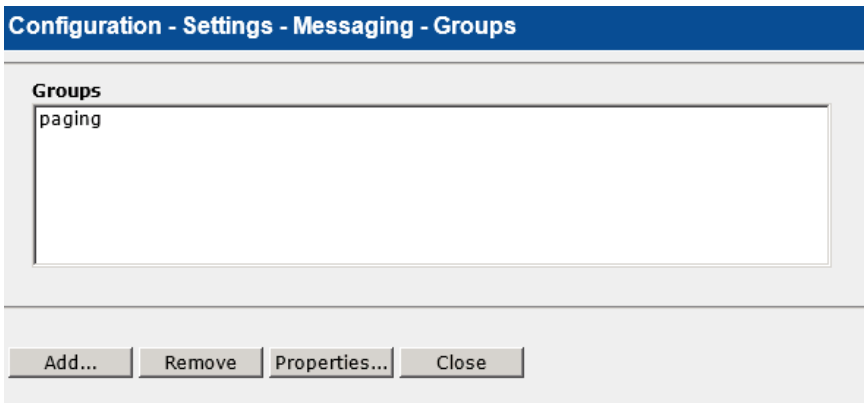
1. From the **Configuration - Settings - Messaging - Devices** window highlight the device you want to edit
2. Click **Properties**
3. The **Name** or **Description** can be changed, the Number cannot
4. Click **Save**

To remove a Messaging Recipient:

1. From the **Configuration - Settings - Messaging - Devices** window highlight the messaging recipient you want to remove
2. Click **Remove**
3. The **Remove** dialog box appears to confirm that you want to delete the specified messaging recipient.
4. If you are sure that you want to remove the recipient, click **OK** otherwise click **Cancel**

Groups

In order for similar messages to go out to a group of Messaging Devices, you must configure Messaging Groups. Use the following steps to add, edit, and remove messaging groups as well as configure which alarms are sent to the group.

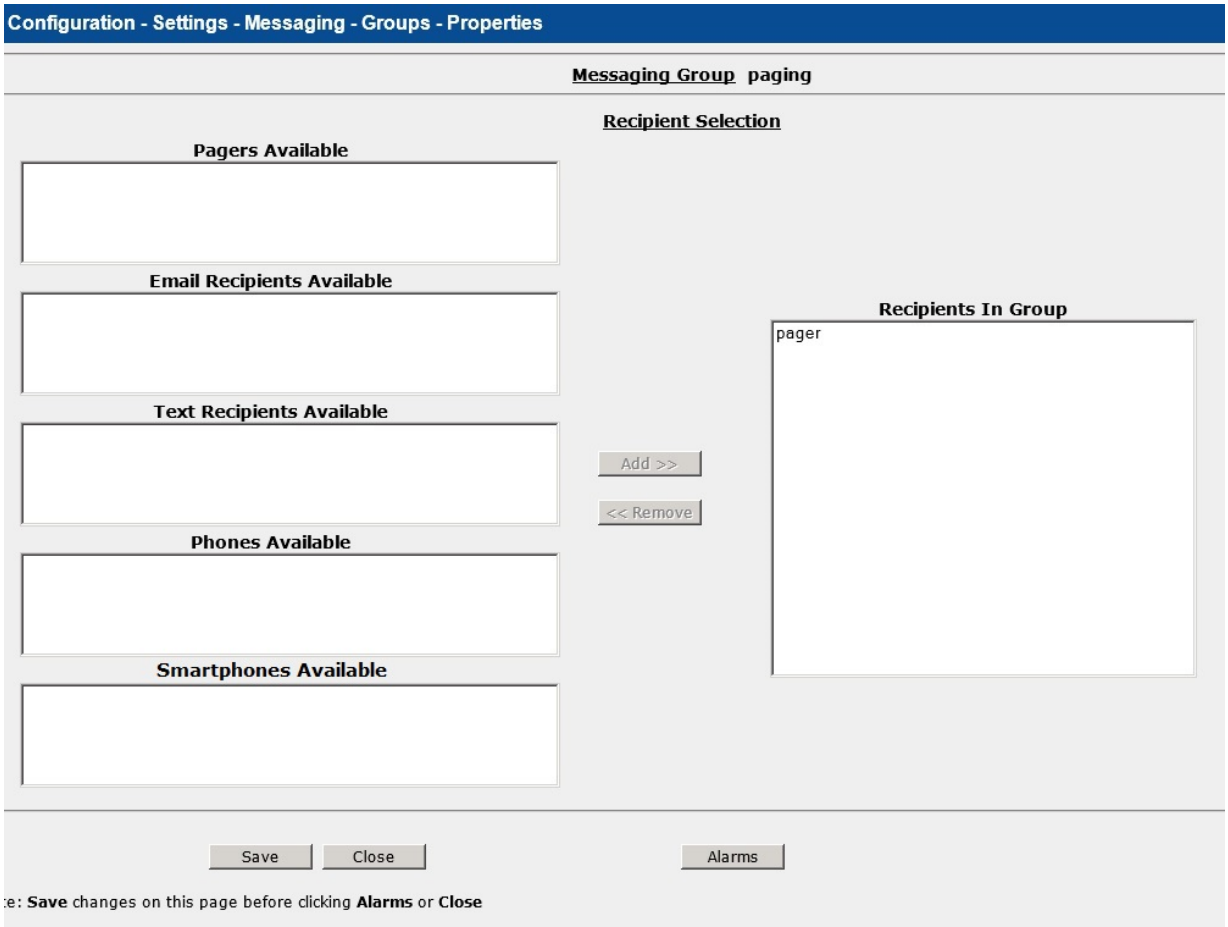


To add a Messaging Group:

1. From the **Messaging** page, click the **Groups** link
2. Click **Add…**
3. Type a **Name** for the Group
4. Click **Save**
5. The group you added appears in the Messaging Groups window

To add Available Devices to a messaging group:

1. From the **Configuration - Settings - Messaging – Groups** window, highlight a Messaging Group
2. Select **Properties…**
3. The **Configuration – Settings – Messaging – Groups - Properties** window opens for the selected group



4. In the applicable **Available** field, click on the item you want to add
5. Click **Add >>**
6. The available item appears in the **Recipient In Group** field
7. Click **Save** to save your changes and return to the Messaging Groups window or click **Close** to disregard the changes made
8. To configure **Alarms**, refer to Configuring Alarms and Events for Messaging Groups

To remove Available Devices from a messaging group:

1. From the **Configuration - Settings - Messaging – Groups** window, highlight the Messaging Group from which you want to remove the device
2. Select **Properties…**
3. In the **Recipient In Group** field, highlight the recipient you want to remove
4. Click **Remove**
5. The recipient appears in the applicable **Available** field
6. Click **Save** to save your changes and return to the Messaging Groups window or click **Close** if you do not wish to save your changes

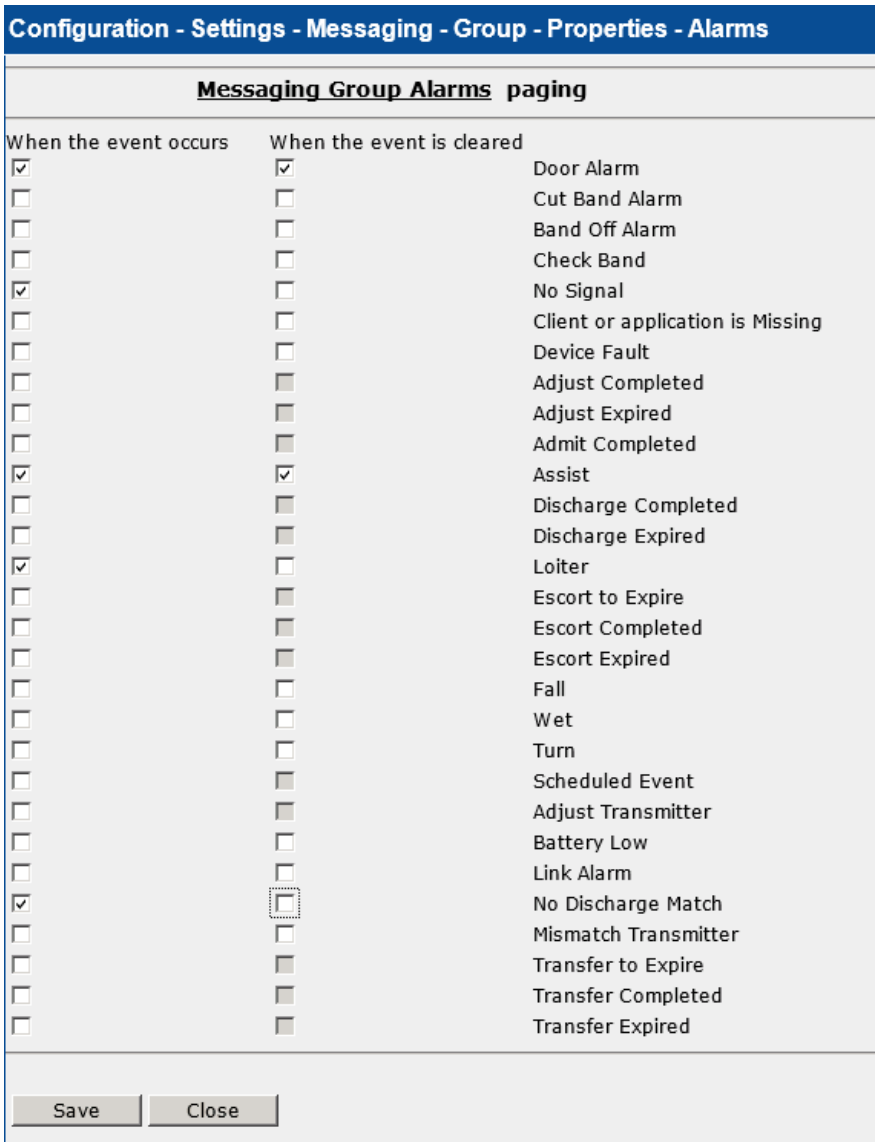
Alarms and Events

The Alarms option in the Messaging Group window allows you to select which alarms and events you want to trigger a message to certain messaging groups. You can send a message to a group when certain events occur, or you can send a message to a group when certain events are cleared.

For example, at your facility Security Guards may only need to be messaged in the event of a Cut Band Alarm or Door Alarm. You can use the Alarms option in the Messaging Group window to specify those settings for that specific messaging group.

To configure Alarms and Events for messaging groups:

1. From the **Configuration - Settings - Messaging – Groups** window, highlight the group to which you want to configure the alarms and events
2. Select **Properties…**
3. Click **Alarms**



4. In the **When the event occurs** field, select the checkboxes for those specific alarms/events for which you want messages sent (when the alarm/event occurs)
5. In the **When the event is cleared** field, select the checkboxes for those specific alarms/events for which you want messages sent (when the alarms/event is cleared). Event cleared may only be checked if the associated **When the event occurs** box is checked
6. Click **Save** to save your changes and return to the Messaging Groups window

Alarm/Event	Explanation of Alarm/Event
Door Alarm	A door is open with an alarming band or Wanderer transmitter in the Exit Alarm Zone.
Cut Band	The banding material was cut or tampered with on an alarming band transmitter.

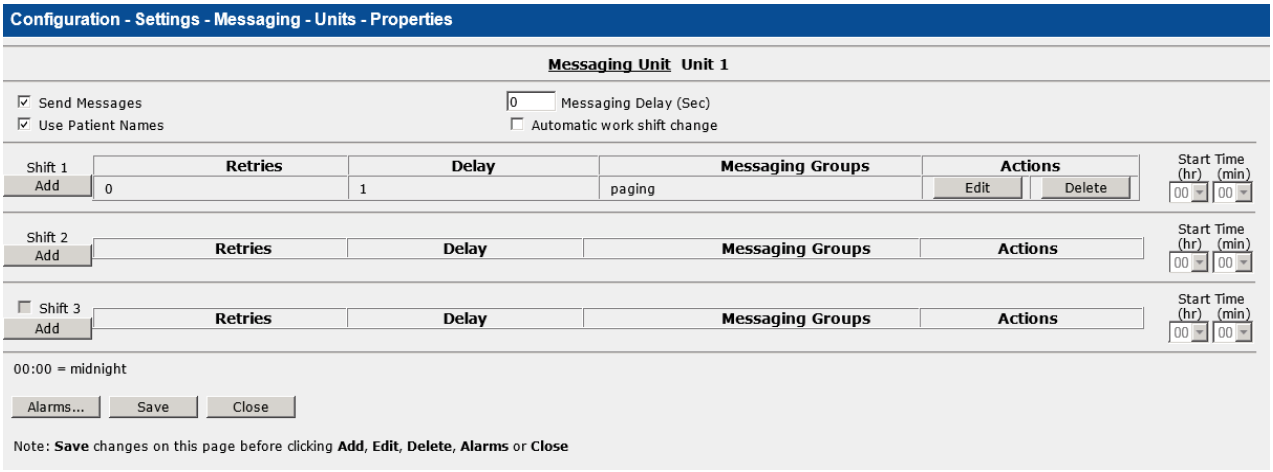
Band Off Alarm	The transmitter and/or band have come off of the infant patient.
No Signal	A transmitter needs to be checked. This alarm is generated when an alarming band transmitter, QR Plus transmitter or QR Premiere transceiver fails to check-in with the system.
Client or application is missing	A Client computer or service is no longer communicating with the system.
Device Fault	A Device in the system is not responding to the software or not functioning properly.
Adjust Completed	An Adjust function has completed properly.
Adjust Expired	An Adjust function has expired.
Admit Completed	An Admit function has completed properly.
Assist	An Assistance Required alarm has occurred (QR Plus, 9500 and QR Premiere only).
Discharge Completed	A Discharge function has completed properly.
Discharge Expired	A Discharge function has expired.
Loiter	A person with an Infant, Smart Sense, Wanderer or Code Watch transmitter remains in range of a monitored door for longer than the Loiter delay.
Escort to Expire	An Escort function in process is about to expire.
Escort Expired	An Escort function has expired.
Escort Completed	An Escort function has completed properly.
Fall	Weight is removed from the sensor pad.
Wet	Fluid is detected on an incontinence pad.
Scheduled Event	The time set for a scheduled event has occurred.
Adjust Transmitter	A band slippage check, which occurs one time only, is issued based upon the time configured.
Battery Low	A transmitter has a low battery.
Link Alarm	There is a problem linking the Infant transmitter to a Mother or Baby Check transmitter.
No Discharge Match	An infant is discharged and the banding material on the Infant transmitter is cut before performing the required mother/infant match.
Mismatch Transmitter	An infant transmitter is located within proximity of a Mother or Baby Check transmitter that is linked to a different infant transmitter.
Transfer to Expire	A Transfer function in process is about to expire.
Transfer Completed	A Transfer function has completed properly.
Transfer Expired	A Transfer function has expired.

NOTE: Any device not assigned to a unit, in addition to devices that cannot be assigned to a unit (repeaters), belong to the Auto-Enroll unit. Only paging groups assigned to this unit will be sent event information related to those devices. Client Missing alarm messages will only be sent to messaging devices that are assigned to the Auto-Enroll Unit.

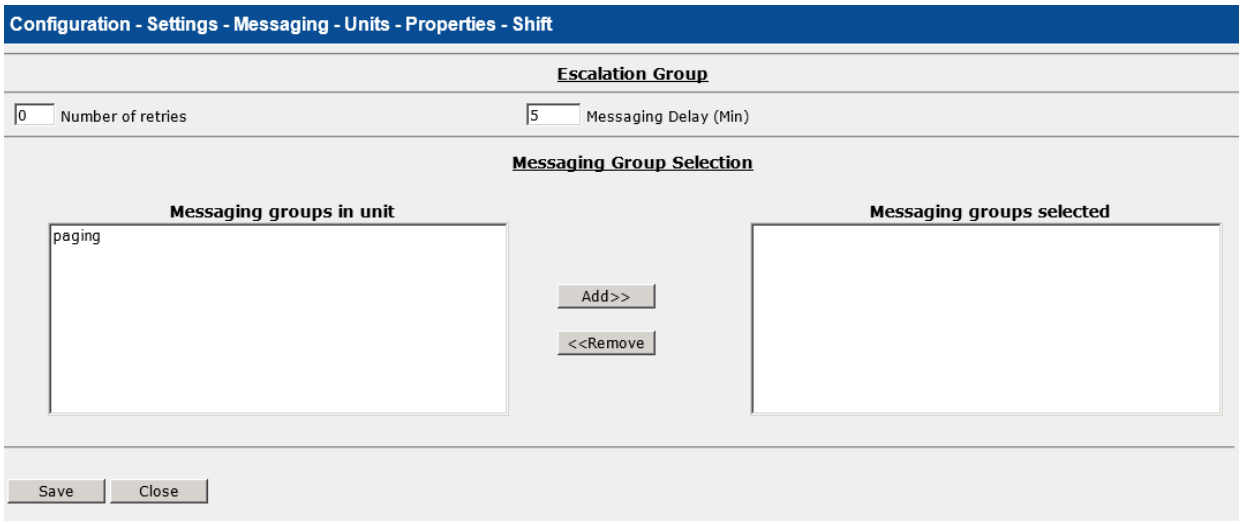
Units In order for messages with similar alarms to go out to Messaging Groups within a particular unit, you must configure a Messaging Unit. Use the following steps to add, edit, and delete Messaging Units as well as configure which alarms message a specific Messaging Unit.

To configure a Messaging Unit:

1. From the **Messaging** page, click the **Units** link
2. The **Configuration - Settings - Messaging - Units** window opens with a list of the units already configured in the system
3. Highlight the unit you want to add Messaging Groups to
4. Click on **Properties…**



5. If you want the system to send messages for this Messaging Unit, click the **Send Messages** checkbox
6. If you want the system to use names of the patients whose transmitter/device triggered the messaging alarm, click the **Use Patient Names** checkbox
7. In the **Messaging Delay** field, specify the amount of seconds you want the system to wait before it begins messaging, to allow for location information to be acquired
8. Click **Save** to save your changes
9. Starting with **Shift 1**, click **Add** to specify the initial messaging group(s) or the messaging escalation group(s) for the shift
10. The **Configuration – Settings – Messaging – Units – Properties - Shift** window opens. The available Messaging Groups in this dialog box depend on the Messaging Groups that have already been configured in the system. (See Groups)



11. In the **Number of retries** field, enter how many times you want the system to message a Messaging Group before escalating the message to another group
12. In the **Messaging Delay** field, enter how many minutes you want to pass before messaging retries
13. In the **Messaging groups in unit** field, highlight the messaging group you want to add
14. Click **Add>>**
15. The selected group appears in the **Messaging groups selected** field
16. Click **Save** to save your changes and return to the Messaging Units window
17. If applicable, repeat the same steps to add additional escalation groups
18. On the Messaging Unit screen, the unit's alarms must be enabled for the Messaging Unit to function
19. Select the **Alarms…** button and check the alarms that the Messaging Groups in this Unit receive. (See Explanation of Alarms and Events)

NOTE: If no alarms are selected, the system will send out messages based upon the alarm selected in the individual Messaging Group.

To configure messaging with Shift Changes:

1. From the **Configuration - Settings - Messaging – Units** window, highlight the unit you wish to modify
2. Select **Properties**
3. Select the **Automatic work shift change** checkbox
4. Work Shift 1 and Shift 2's start times become enabled
5. If your facility has 3 work shift changes, select the Shift 3 checkbox
6. In the **Start Time** field, from the pull-down list, select what time each shift begins
7. Click the **Add** button below Shift 1
8. In the **Number of retries** field, enter how many times you want the system to message a group before escalating the message to another group
9. In the **Messaging Delay** field, enter how many minutes you want to pass before messaging retries
10. In the **Messaging groups in unit** field, highlight the message group you want to add
11. Click **Add>>**
12. Once you are finished with your changes, click **Save**
13. Repeat the same steps to configure Escalation Groups for Shifts 2 and 3

To change the settings of an Escalation Group:

1. From the **Configuration - Settings - Messaging – Units** window, highlight the unit you wish to modify
2. Click on **Properties…**
3. Under the **Actions** field, click **Edit**
4. Make the appropriate changes, and click **Save**

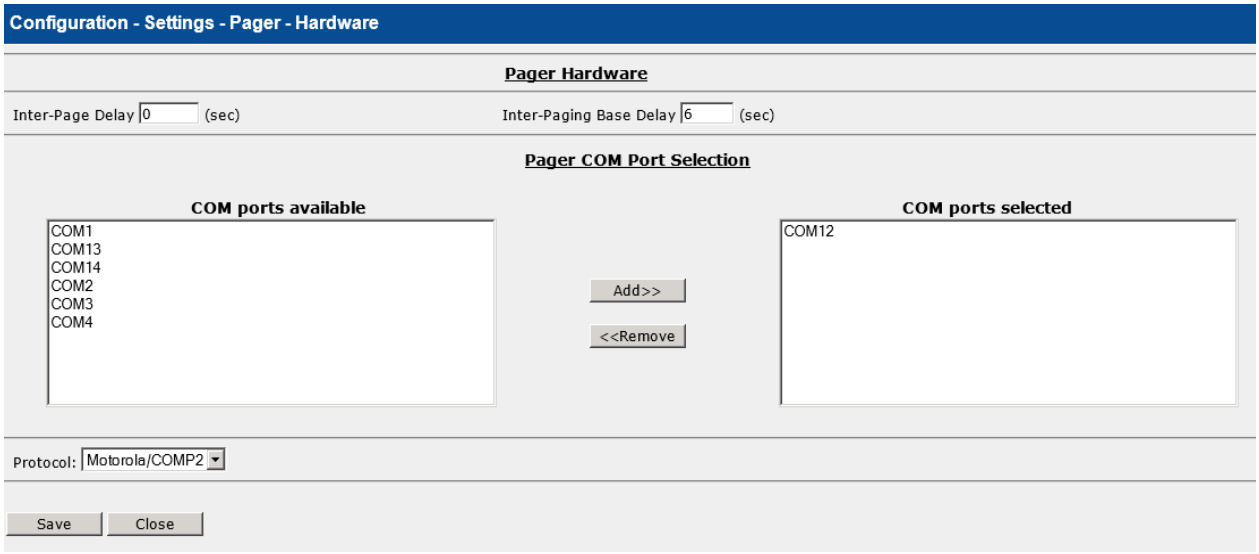
To delete an Escalation Group:

1. From the **Configuration - Settings - Messaging – Units** window, highlight the unit you wish to modify
2. Click on **Properties…**
3. Under the **Actions** field, click **Delete**
4. The Delete Settings dialog box appears to confirm that you want to delete the specified group
5. Click **OK**

Pager Hardware

Using the Pager Hardware option, you can configure specific settings about paging including the pager base serial port and the specific paging protocol your facility uses.

NOTE: The pager base serial port cannot be mapped until a 9450 or Quick Response System is mapped to a communications port.



To configure Pager Hardware:

1. Go to the **Configuration** home page
2. Select **Settings**.
3. Select **Pager Hardware**.
4. In the **Inter-Page Delay** field, enter how many seconds you want to pass between each page
5. In the **Inter-Paging Base Delay** field, enter how many seconds you want to pass before the next paging base starts transmitting. This is a minimum of 6 seconds.
6. In the **COM ports available** field, highlight the pager base COM port you wish to select. A maximum of 4 Paging Bases can be connected at once.
7. Click **Add** and the COM port appears in the **COM ports selected** field
8. Select a page **Protocol** from the pull-down list
9. Click **Save**
10. You must restart the Central Server in order for the system to apply the new settings

EXAMPLE: System has Multiple Paging Bases

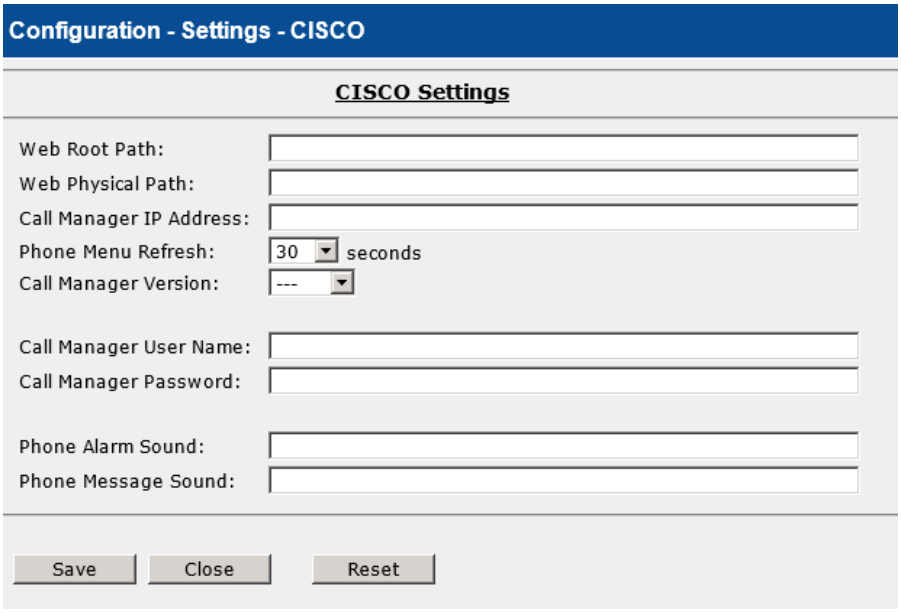
If the system has 2 paging bases connected and there are 2 pagers receiving messages, the message output will be as follows:

- Two alarms are generated at the same time
- Alarm 1 is sent to pager 1 via Paging Base 1. Then, Alarm 1 is sent to pager 1 via Paging Base 2
- Alarm 1 is sent to pager 2 via Paging Base 1. Then Alarm 1 is send to pager 2 via Paging Base 2
- Then, Alarm 2 is sent to pager 1 via Paging Base 1, then to pager 1 via Paging Base 2
- Finally, Alarm 2 is sent to pager 2 via Paging Base 1, then to pager 2 via Paging Base 2

CISCO Settings

The Cisco Messaging Interface is designed to provide mobile event notification, mobile event classification and hands free voice-to-voice communications between the care giver and patient. Cisco Settings allow you to configure the Cisco interface

NOTE: When you are done configuring the Cisco settings, you **MUST** restart the Central Server in order for the system to apply the new settings.



- **Web Root Path**: The path to web configuration using the IP address instead of the server name. **NOTE**: The path MUST contain the ending "/" slash

  For example: *http://192.168.1.254:9185/WardenConfig/*

- **Web Physical Path**: The location on the hard disk of the web configuration files. **NOTE**: The path MUST contain the ending "\" slash

  For example: *c:\apache-tomcat\webapps\WardenConfig*
- **Call Manager IP Address**: IP address of the Cisco Unity Communications Manager (CUCM)
- **Phone Menu Refresh**: The frequency that a phone will re-display active alarms.
- **Call Manager Version**: The version of Call Manager that the RFT Server is interfacing to (CM4, CM6, CM10 or CME). When the RFT Cisco IP Phone Service starts up, it will not send alarms to the phone until it has read the service and system configuration. When configured for CM4, CM6 or CM10, this requires approximately 30-45 seconds. For CME Servers, the phone configuration may require 2-3 minutes to retrieve.

NOTE: When phone configuration is changed on the CME Server, the RFT Cisco IP Phone Server must be restored.

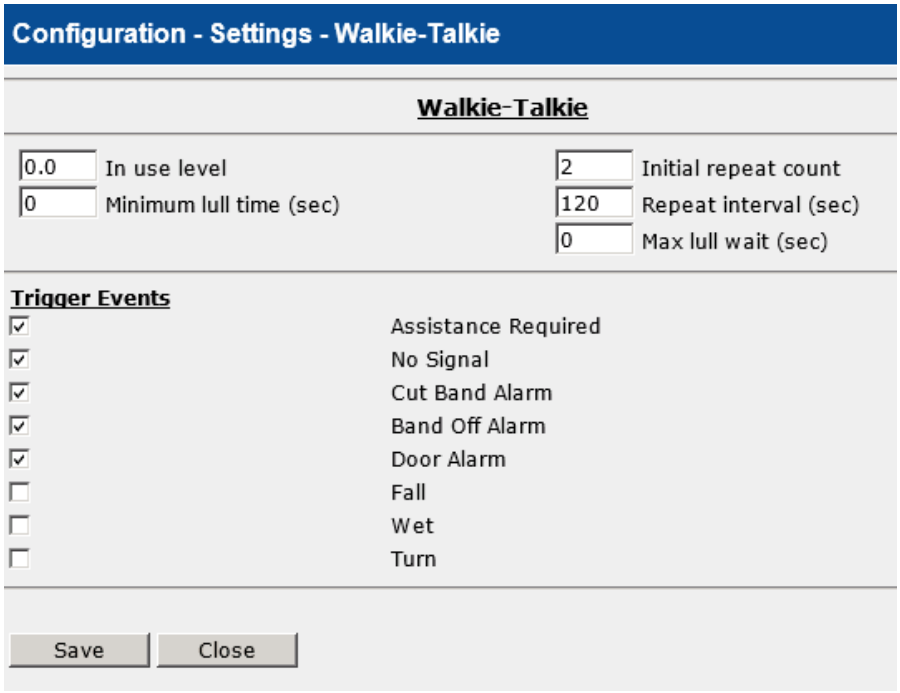
- **Call Manager User Name**: User name defined in CUCM that has rights to submit AXL calls and is associated with the Cisco phones to receive alarms.
- **Call Manager Password**
- **Phone Alarm Sound**:
- **Phone Message Sound**

Walkie-Talkie

Walkie-Talkie alerts staff members when specific events occur. Staff members equipped with a Walkie-Talkie will receive an audible message for triggered events. The options for triggering events are:

- Assistance Required
  - Smoke, Emergency, and CO alarms will also be sent when this option is selected.
- No Signal
  - Check alarms will also be sent when this option is selected.
- Cut Band Alarm
- Band Off Alarm
- Door Alarm
- Fall
- Wet

The Walkie-Talkie system also allows you to set the number of seconds between the start of an alarm and when the alarm is repeated. This is referred to as a repeat interval. The repeat interval countdown starts as soon as the Walkie-Talkie alarm sounds. Therefore, depending on the number of seconds selected for a repeat interval, an alarm may repeat only seconds after the first alarm stops.



To set the Repeat Intervals:

1. Go to the **Configuration** home page
2. Select **Settings**
3. Select **Walkie-Talkie**
4. The Walkie-Talkie window opens, allowing you to set the properties for the Walkie-Talkie. **NOTE**: Before a Walkie-Talkie message is sent, the system listens to the output channel for a lull in voice activity.
   - **In use level**: The RMS noise level at which the output channel is considered in use
     - **Minimum**: 0.0
     - **Default**: 2.0
     - **Maximum**: 2.5
   - **Minimum lull time**: Consecutive seconds the noise level must be under the "In use level" before the channel is considered not in use
     - **Minimum**: 0. The first second that exceeds the In use level ends the lull. If the In use level is not reached, the lull time will be the time defined in Max lull wait.
     - **Default**: 0
     - **Maximum**: 30
   - **Max lull wait**: Maximum time to wait for a lull. After this amount of time, the message will be sent regardless of output channel activity.

- **Minimum**: -1. At this value, there is no lull between messages
- **Default**: 0. There will be a one-second delay between messages.
- **Maximum**: 300

- **Initial repeat count**: Sets the number of times a new message is repeated (walkie-talkies can be set up to repeat a message several times when it first occurs and then have it repeat periodically after that until it clears)
  - **Minimum**: 0
  - **Default**: 2
  - **Maximum**: 99
- **Repeat interval**: Sets how often an active alarm message is repeated.
  - **Minimum**: 0
  - **Default**: 120
  - **Maximum**: 9999

5. With the Walkie -Talkie window still open, select the **Trigger Events**
6. Staff members equipped with a Walkie-Talkie will receive an audible message for events selected.
7. When you are done configuring the Walkie-Talkie, click **Save**
8. You **MUST** restart the Central Server in order for the system to apply the new settings

NOTE: New alarms will not be broadcast until system has finished repeating the original alarm.

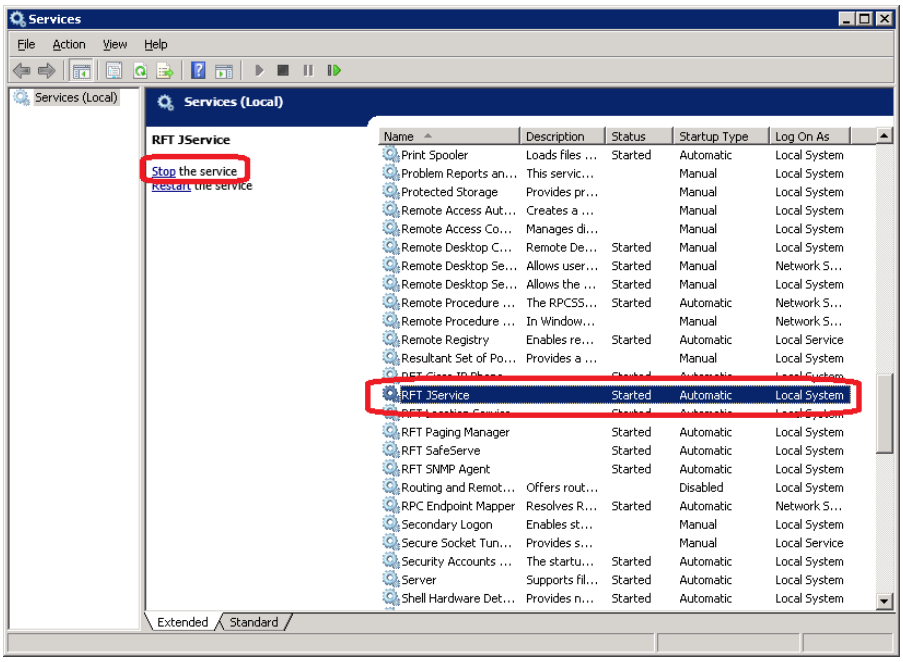
WAV Files

You can change the default WAV files played on the walkie-talkies with your own files by overwriting the default file with a new file of the same name. Before you change the default WAV files, you must stop the RFT JService.

WARNING: Events occurring while the RFT JService is down will not be recorded. Alarming events will continue to generate and display in the software's Client application.

To stop the RFT JService:

1. Go to the Services menu by selecting **Control Panel>> Administrative Tools>> Services**
2. Double click **Services** to open the Services window



3. Scroll through the list and highlight **RFT JService**
4. Select **Stop the service** from the menu on the left
5. Verify that the status no longer states *Started*

To configure the WAV File:

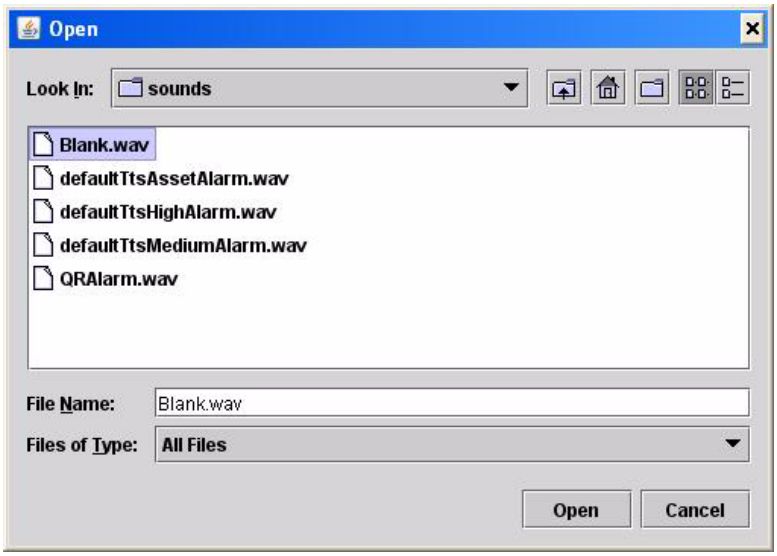
NOTE: You must make sure that no active alarms are in the system before starting this process.

1. From Windows Explorer, navigate to: *C:\Program Files (x86)\RF Technologies\sounds*
2. In this directory, there are three WAV files for controlling the Asset, Medium, and High alarms issued by the Walkie-Talkie:
   - defaultTtsAssetAlarm.wav
   - defaultTtsMediumAlarm.wav
   - defaultTtsHighAlarm.wav
3. Rename the existing WAV file corresponding to the alarm sound you wish to change. For example, rename *defaultTtsHighAlarm.wav* to *original_defaultTtsHighAlarm.wav*
4. Copy your new sound file to the audio directory and rename it to the original name of the file from (in our example, you will want to rename your new WAV file to *defaultTtsHighAlarm.wav*)
5. The next alarm that is issued to your Walkie-Talkie system will use your new WAV file

To blank out the Client Application Sound on the Server :

NOTE: To hear the WAV file played on the Walkie-Talkie, you must blank out the Client application's sound on the Server

1. Go to the **Client Properties** window
2. Click the **Sounds** tab
3. In each of the fields, click **Browse...** to select the location of the **.wav** file that contains the sound to be applied to the alarm
4. Select **Blank.wav**



5. Click **Open** to move the setting to the selected field
6. Click **Save** to save the changes and return to the main window

To restart the RFT JService:

1. Go to the Services menu by selecting **Control Panel>> Administrative Tools>> Services**
2. Double click **Services** to open the Services window
3. Scroll through the list and highlight **RFT JService**
4. Select **Start the service** from the menu on the left.
5. Verify that the status now states *Started*
6. Click on the **X** in the upper right corner to close the Services window

Locations

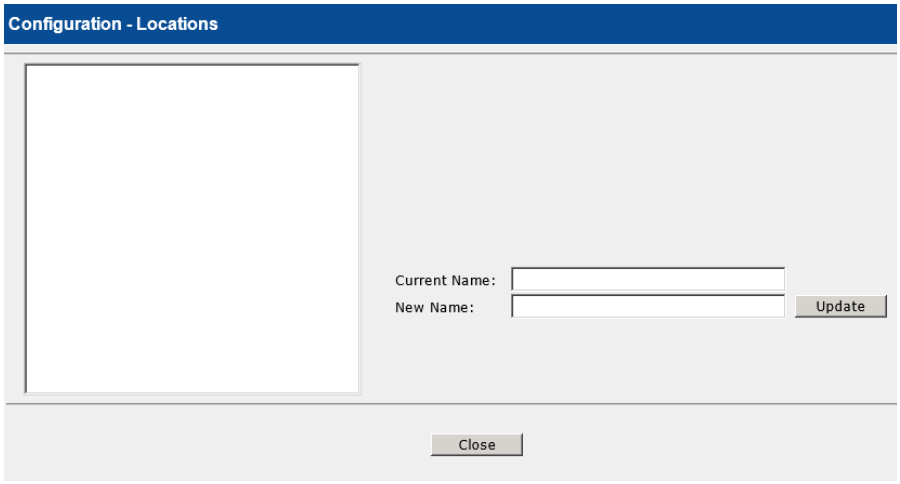
When a location database has been installed on the Server, the list of detailed location names defined for the Quick Response Plus Location Engine is presented via web configuration. If names change in the future, web configuration also supports renaming a location to reflect its new name.

As an example, if the location currently known as the “East Patio” has been given a new name of “Sunrise Garden”, the name should be changed in the location database for pendant events to reduce confusion for the staff and caregivers.

NOTE: The text fields for the Configuration Locations window will be empty if you are licensed for Quick Response Plus and Smart ID, and the Use Location Engine For Pendant Alarms checkbox is unchecked (refer to Global Settings). It will also be empty if the Use Location Engine For Pendant Alarms checkbox is checked and you do not have any locations.

To change the name of a Location:

1. Go to the **Configuration** home page
2. Select **Location**

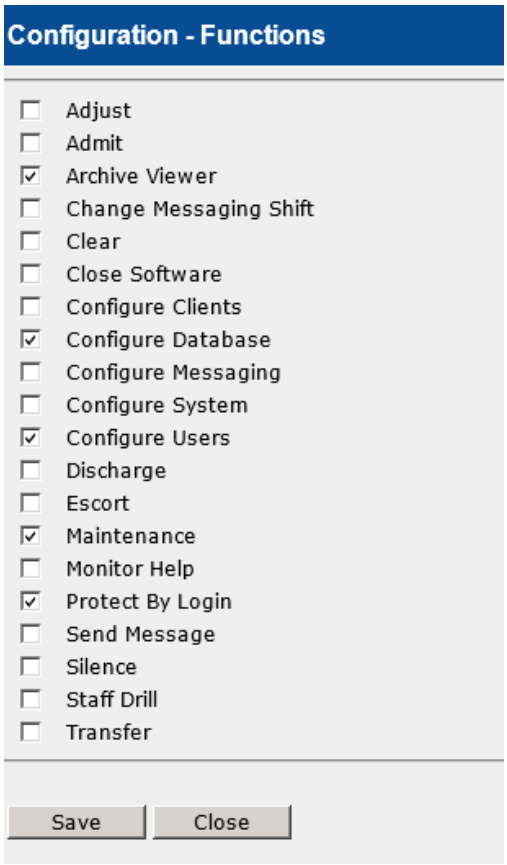


3. Scroll through the list of location names
4. Select the location name to change
5. Type the **New Name** of the location in the text field to the right
6. Verify that the selected location name and the new location name are both correct
7. Click **Update** to save the new name for the selected location
8. Repeat for other locations as necessary

Functions

Many of the functions available in the software can be protected by a password. If a function is password protected, users are required to both swipe their identification card and enter a password, or enter their login and password (depending upon your LDAP configuration) in order to access the window(s) in which they can perform the desired function.

NOTE: Password protection is a system-wide setting; all Client computers are subject to the same password requirements.



To Protect the system with passwords:

1. Go to the **Configuration** home page
2. Select **Functions**
3. Select what function is to be protected by a password by clicking the checkbox next to the desired function(s)
4. Click **Save** to save and return to the main window

Function	Explanation
Admit	Allows you to admit a patient in the software
Adjust	Allows you to temporarily suspend the alarm function for a patient or asset's alarming band transmitter so the banding material can be readjusted Function only applies to system licensed for Safe Place using 9450 transmitters.

Function	Explanation
Archive Viewer	Allows you to create a report of archived data for viewing.
Change Messaging Shift	In some cases, it may be necessary to change a page unit's work shift. This feature allows you to select a different messaging unit and work shift.
Clear	An event is an alarm that occurs in the software that usually requires an authorized user to enter an event cause to clear the alarm.
Close Software	Allows you to exit the software application.
Configure Clients	Allows you to configure Client Properties as well as access the Configuration Client and Configuration Causes windows.
Configure Database	Allows you to access Configuration Global Settings, Transmitter ID Ranges, Card Reader Strings, Units, Rooms, and Devices.
Configure Messaging	Allows you to configure messages, pager, email, Cisco, smartphone, and walkie-talkie settings.
Configure System	Allows you to access Server Management where you can scan and reset devices, lock and unlock a global lockdown, configure Poll Server Settings, Noise Analysis, view the Dashboard, and view the list of installed RFT Software files.
Configure Users	Allows you to configure the system users and their assigned functions.
Discharge	Allows you to take a patient or asset out of the census of monitored transmitters.
Escort	Allows you to select the amount of time required to take a patient or asset out of a protected area and back to the same protected area.
Maintenance	Allows you to manually enter a log of maintenance performed on the system in the System Maintenance window. This information is then available in the System Maintenance Report.
Monitor Help	Allows you to view specific on-line help and track the identification of the viewer so that training needs can be determined.
Pre-Enroll	Allows you to allocate transmitters to specific patients before admission. Function only applies to systems licensed for Safe Place using 9450 transmitters.
Protect By Login	Allows you to specify which users may change the password protected functions listed on this page.
Send Message	In some cases, it may be necessary to send a manual message to a staff member. This feature can only be used if your system is configured for messaging.
Silence	Allows you to stop the alarm sound at the computer. The alarm is silenced for the configured length of time; however, the event still appears in the Event List.
Staff Drill	When a staff drill is requested, the attendant performing the drill can manually enter the information in the Staff Drill window. This information is then available in the Staff Drill Report.
Transfer	Allows you to select the amount of time required to move a patient or asset from one protected area to another protected area.

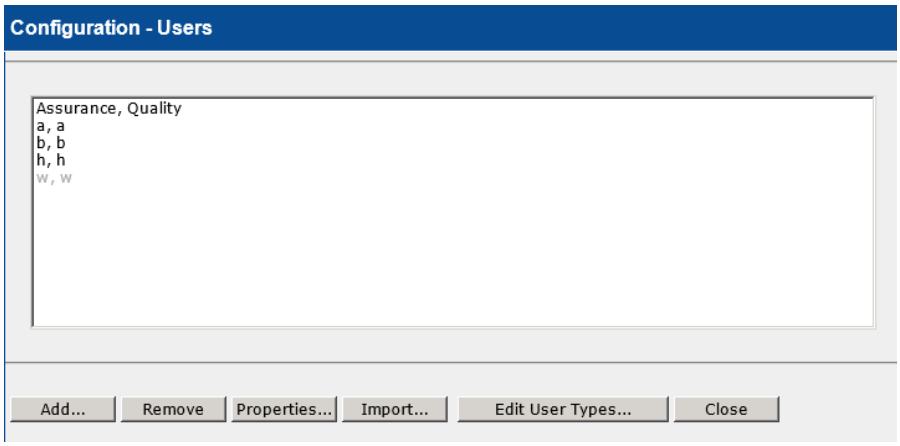
Users

Users of the system and their assigned functions are configured from the Users link.

Adding a User

To add a User:

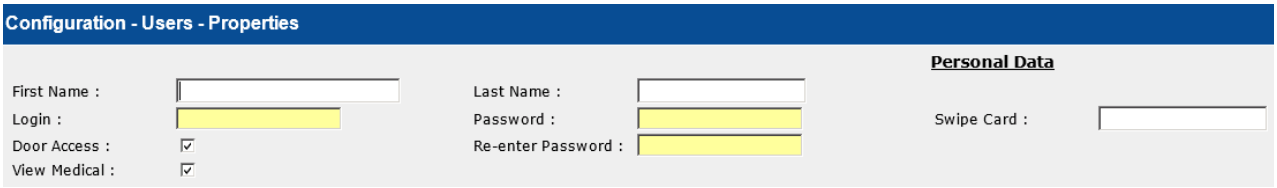
1. Go to the **Configuration** home page
2. Select **Users**



3. Click **Add**
4. The **Configuration – Users - Properties** window opens with options to enter personal data, contact data, and assign functions for the user

Personal Data

In the Personal Data section, enter general information about the user being added



- **Login**
- **Password**
- **Swipe Card**
- **Re-enter Password**

NOTE: The Login, Password and Swipe Card information is case sensitive. It is recommended that you turn off the Caps Lock on your keyboard before entering this information.

CAUTION: If utilizing LDAP authentication, it is recommended that when creating a user account, use a "dummy" password. The password **cannot** contain any of the following characters: **" * + , / ? : ; < = > [ ] \ |**

These characters have special meaning within the software database structure. This password simply allows you to create the user account but will not be used to login to the system. This should be done **prior** to enabling LDAP authentication. Once LDAP authentication is enabled (refer to the *Authentication* section for additional details), the software will use the active directory system password already assigned to the user so users just need to login to the software using their windows password.

- **Door Access**: Check the checkbox to allow the user to use their magnetic or proximity identification card at the door. This function is limited to 256 users.
- **View Medical**: Check the checkbox to allow the care giver to view the Medical Info tab during the admit process.

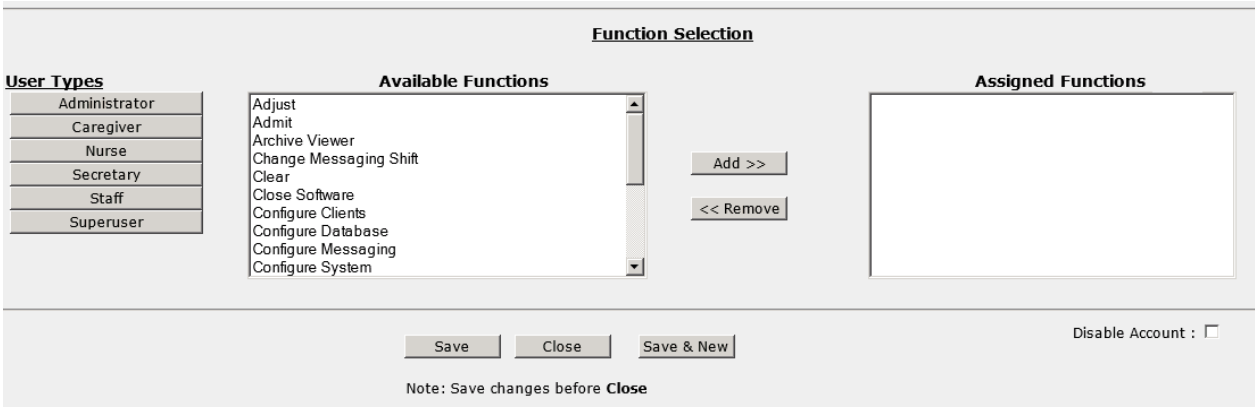
Contact In the Contact section, enter contact information about the user

- For text messaging: Type the user's **Email** address, **Phone** number and **Text** address (email address)

Function Selection In the Function Selection section, select the functions allowed to the user.

Functions/permissions allowed to the user can be quickly assigned by selecting a **User Type** (see Appendix A for additional details) with those functions already setup or you can manually assign user functions in the **Available Functions** field by highlighting the functions allowed to the user and clicking **Add>>**

If you wish to disallow a function, highlight the function from the **Assigned Functions** field and click **<<Remove**



NOTE: Users assigned the function, "*Receive High Risk Admit Emails*" must have their email address entered in the Contact, Email field.

- **Disable Account**: Click the checkbox to disable a user. Users can be disabled manually or the system can disable a user when the configured Maximum Invalid Logins are reached. Un-checking the checkbox allows the System Administrator to enable a user whose account has been disabled.

NOTE: When disabling a user who will not be returning, make sure to uncheck **Door Access** under the Personal Data section before clicking the **Disable Account** checkbox. Any access card assigned to this user will no longer be sent to door controllers, and will no longer count against the 256 card limit.

Removing a User

To remove a User:

1. Go to the **Configuration Users** window
2. Highlight the user you wish to remove
3. Click **Remove**
4. A dialog box appears asking if you are sure you want to delete the user.
5. Click **OK** to remove from the User list

Viewing User Properties

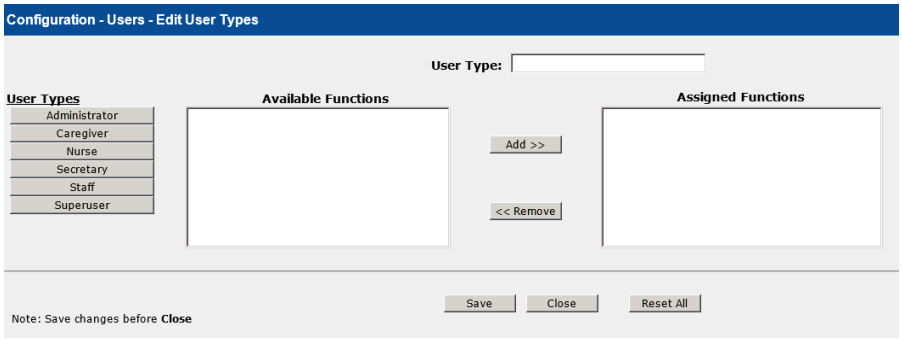
To view User Properties:

1. From the **Configuration - Users** window, highlight the user you wish to view
2. Click **Properties…**
3. The **Configuration - Users - Properties** window opens with that user's information

Editing User Types

To edit User Types:

1. From the **Configuration - Users** window, highlight the user you wish to view
2. Click **Edit User Types…**



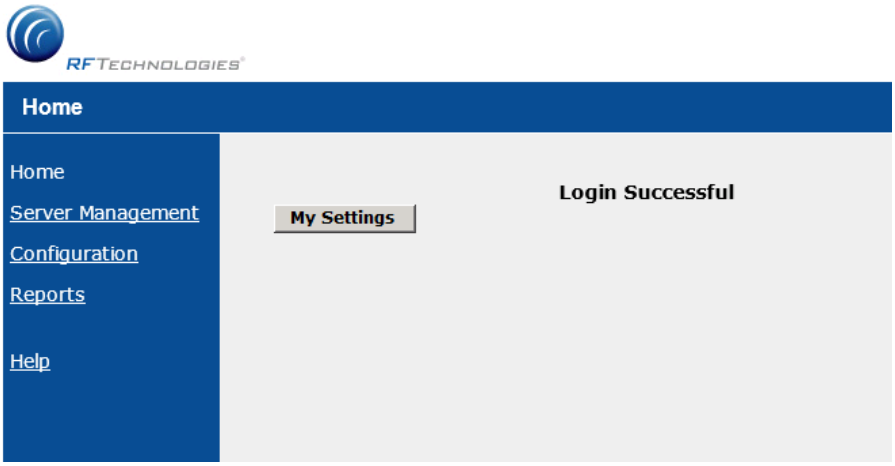
3. Under **User Types**, select the position of the user you want to edit
4. In the **Available Functions** field, highlight the functions allowed to the user and click **Add**
5. If you wish to disallow a function, highlight the function from the **Assigned Functions** field and click Remove
6. Click **Save** to save your changes
7. Click **Reset All** to reset the functions to the default settings

My Settings

Once a user has been set up with a login and password, his/her properties can be viewed from the Home page if the login is successful.

To access My Settings:

1. **Login** then select **Administrative Functions**
2. Select **Configuration**, or double-click the desktop icon if the Client application is not running
3. Click **My Settings** to open the **Configuration - User - Properties** window for your settings

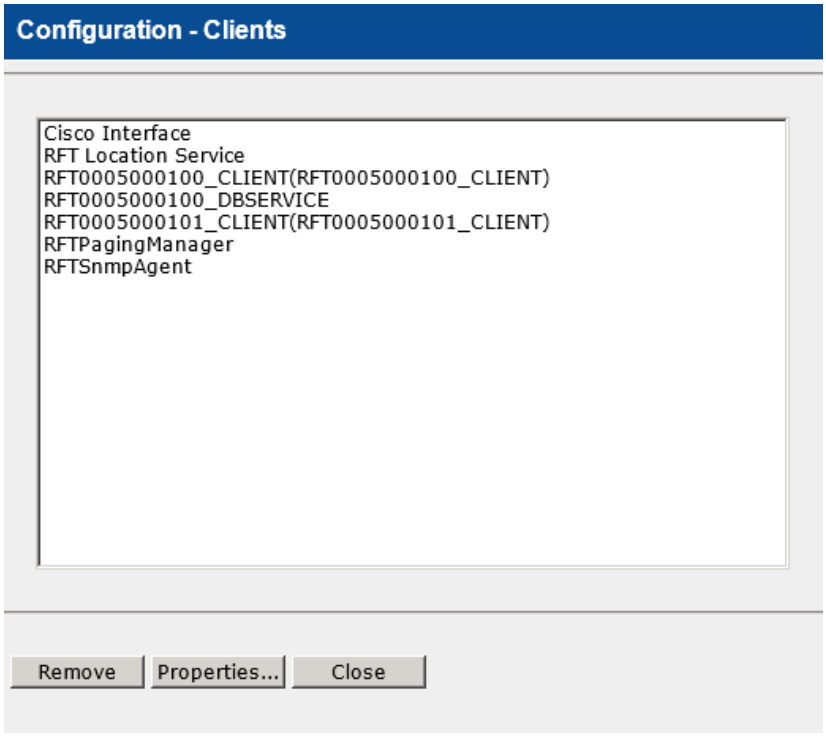


Clients

Depending on your configuration, the system can include several Client computers. The naming convention of the Client computers is determined by RF Technologies and may be confusing to the user. The Clients window allows you to create an alias name that makes the Client computer identifiable to the user. This option also allows you to remove a Client computer.

To create an Alias:

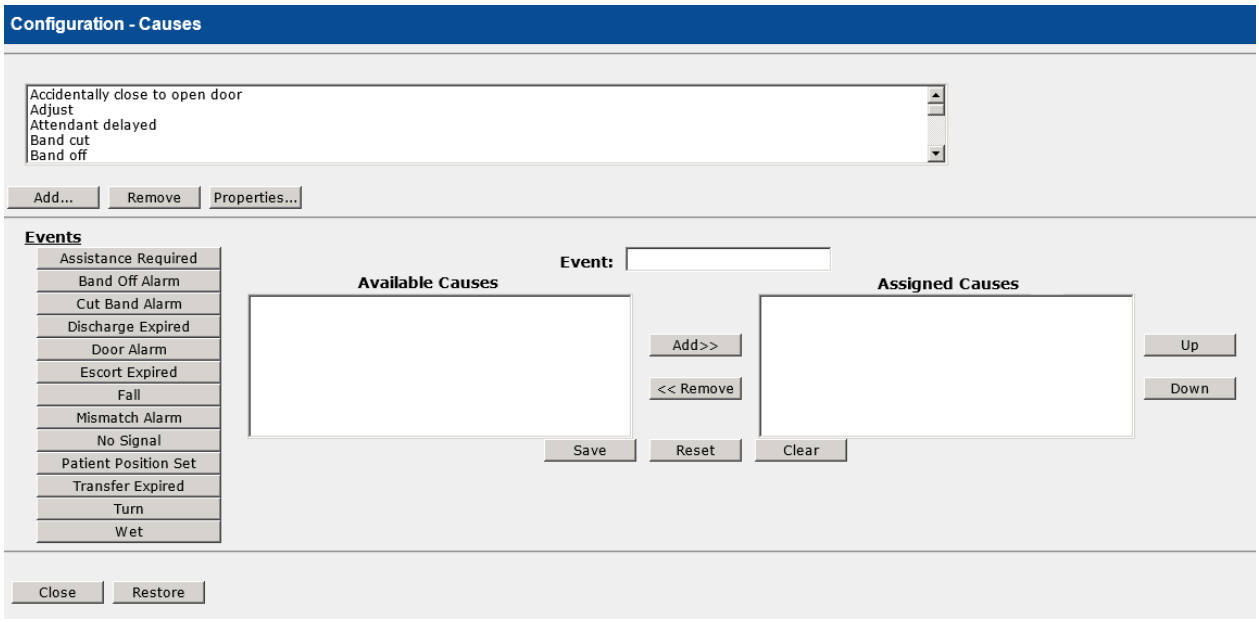
1. Go to the **Configuration** home page
2. Select **Clients**
3. The **Configuration - Clients** window opens



4. Highlight the Client you want to edit
5. Click **Properties…**
6. In the **Alias** field, enter an alias name for the Client computer
7. Choose to have the Client **Auto Close Software** (**NOTE**: When changing the Client application to Auto Close Software, you must restart the Client application for the change to take effect)
8. Select **Save**
9. The **Configuration - Client** window opens with the alias displayed next to the default Client name
10. Click **Close**

Causes

An event is an alarm that occurs in the software that usually requires an authorized user to enter an event cause to clear the alarm. The Configuration Causes window allows you to add, remove or rename event causes. Additionally, you can customize the causes used to clear specific events.



Adding a Cause

To add a Cause:

1. Go to the **Configuration** home page
2. Select **Causes**
3. Select **Add**
4. In the **Name** field, enter an event cause.
5. Click **Save** to save and return to the Causes window. The cause entered will display in alphabetical order in the Causes list.

Removing a Cause

To remove a Cause:

1. Go to the **Configuration** home page
2. Select **Causes**
3. Highlight the cause you wish to remove
4. Click **Remove**
5. The window will refresh with the change.

NOTE: Only event causes that you entered can be removed; default causes cannot be removed.

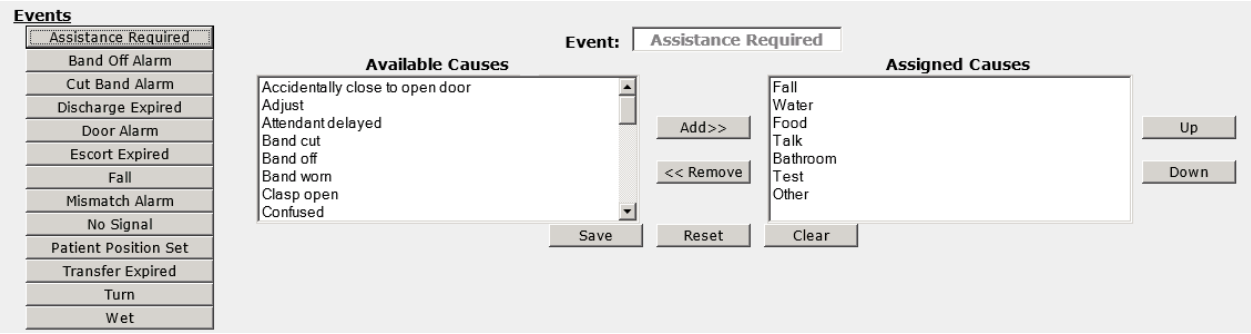
Renaming a Cause

To rename a Cause:

1. Go to the **Configuration** home page
2. Select **Causes**
3. Highlight the cause you wish to rename
4. Click **Properties…**
5. In the **Name** field, rename the event causes
6. Click **Save** to save and return to the Causes window. The renamed cause will display in alphabetical order in the Causes list.

Configuring Causes in Events

You can customize the causes used to clear specific events.



To customize Causes in Events:

1. Go to the **Configuration** home page
2. Select **Causes** to access the **Configuration - Causes** window
3. In the **Events** section of the window, select an event (for example, Assistance Required)
4. The **Available Causes** field populates with all the causes available
5. The **Assigned Causes** field displays the default causes for the alarm event
6. In the **Available Causes** field, select a cause you want to add to **Assigned Causes**
7. Click **Add**; the cause moves to the **Assigned Causes** list. The list allows a maximum of seven causes in addition to Other
8. If you want to remove a cause, select the cause you want to remove and click **Remove**
9. Click **Save** to clear the list and save your changes
10. Click **Reset** to reset the default causes
11. Click **Clear** to clear both the Available Causes and the Assigned Causes Event list
12. When you are done with configuration, click **Close** to exit the window or **Restore** to restore default settings
13. You must restart the Central Server in order for the system to apply the new settings

Maintenance

Once your settings have been configured, the Maintenance window allows you to archive (save) your configuration or restore from a saved configuration. Additionally, you can transfer a person or asset to a new unit or delete the person or asset from the system.

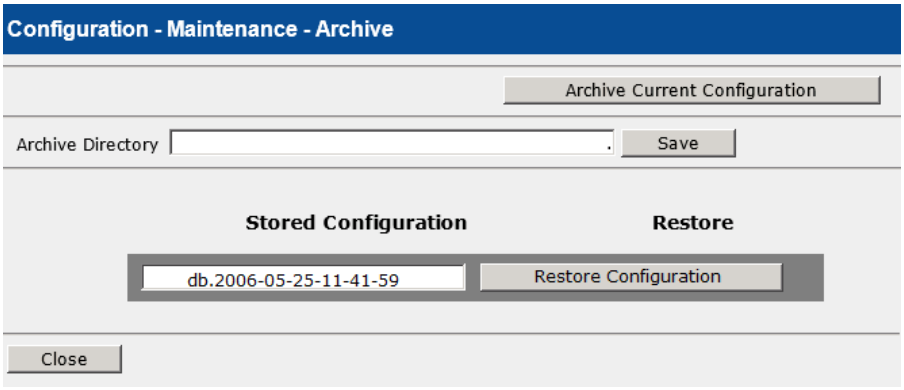
Archive

The configurations you set, according to the standards of your facility, can be stored in an Archive Directory.

NOTE: All Client applications MUST be closed before beginning the Archive process.

To Archive your settings:

1. Go to the **Configuration** home page
2. Select **Maintenance**, and then select **Archive**



3. In the **Archive Directory** field, enter a name for the set of configurations you are storing
4. Click **Save**
5. Click **Archive Current Configuration** to store the current set of configuration in the system's database. This process may take several minutes to complete.
6. Once complete, an Archive Successful or Archive Failure window opens, click **Close** to acknowledge the results. You will be returned to the Login screen to re-launch the Configuration application. The status of the archive now displays in the Archive window.

NOTE: If the application does not re-launch in a couple of minutes, your computer may need to be restarted.

To Restore a configuration:

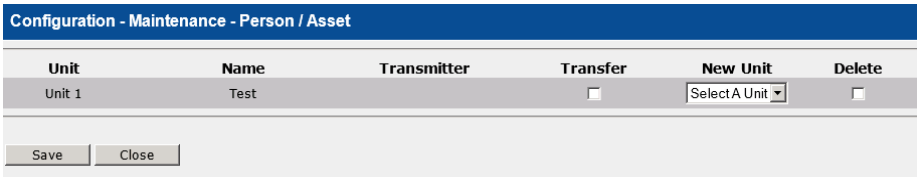
1. Go to the **Configuration** home page
2. Select **Maintenance**, and then select **Archive**
3. Click the **Restore Configuration** button next to the directory that you wish to restore. This process may take several minutes to complete.
4. Once complete, an Archive Successful or Archive Failure window opens, click **Close** to acknowledge the results. You will be returned to the Login screen to re-launch the Configuration application.
5. If the application does not re-launch in a couple of minutes, your computer may need to be restarted.

Person / Asset

If a transfer or discharge did not complete properly, you may use the Person/Asset Tagged Maintenance area to either reassign the patient or asset to a new unit, or remove the patient or asset from the computer manually.

To perform Person/Asset maintenance:

1. Go to the **Configuration** home page
2. Select **Maintenance**, and then select **Person/Asset**



3. Find the Person/Asset for which the maintenance is being performed.
4. Click the **Transfer** checkbox and select a **New Unit** from the pull-down list to transfer the Person/ Asset
5. Click the **Delete** checkbox to delete the Person/Asset from the system
6. Click **Save** to perform the function

Reports

The Reports option allows you to create Archive Viewer reports of archived data for viewing and Unit Detail Viewer reports of devices in a unit.

To access the Reports home page:

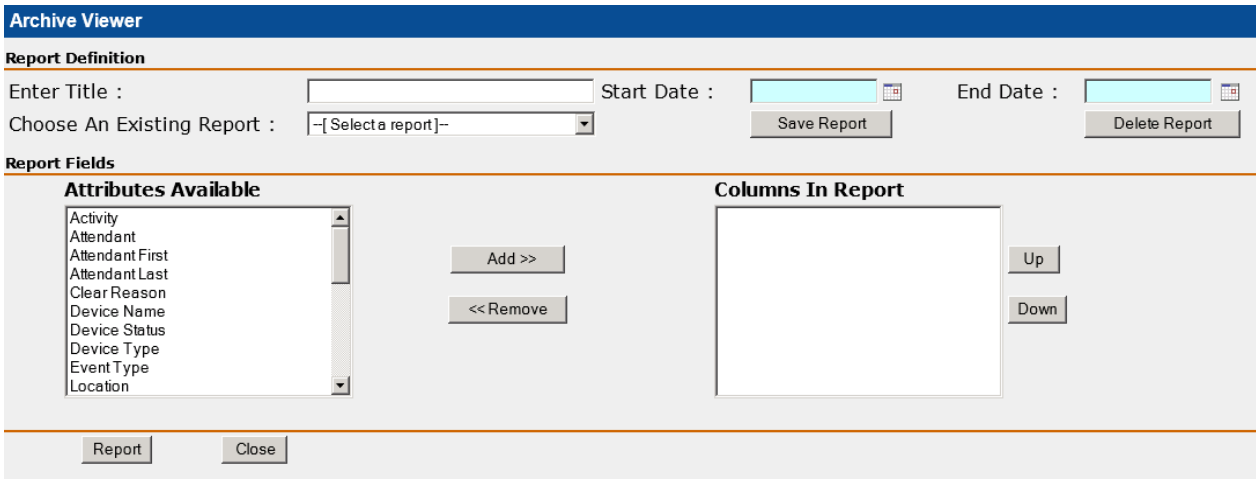
1. **Login** then select **Administrative Functions**
2. Select **Configuration**, or double-click the desktop icon if the Client application is not running
3. Select **Reports**
4. The Reports page opens with links to all the available Reports

Archive Viewer

Archive Viewer allows administrators to create a report of archived data for viewing.

To access the Archive Viewer :

1. From the **Reports** home page, select **Archive Viewer**
2. The **Archive Viewer** window opens.



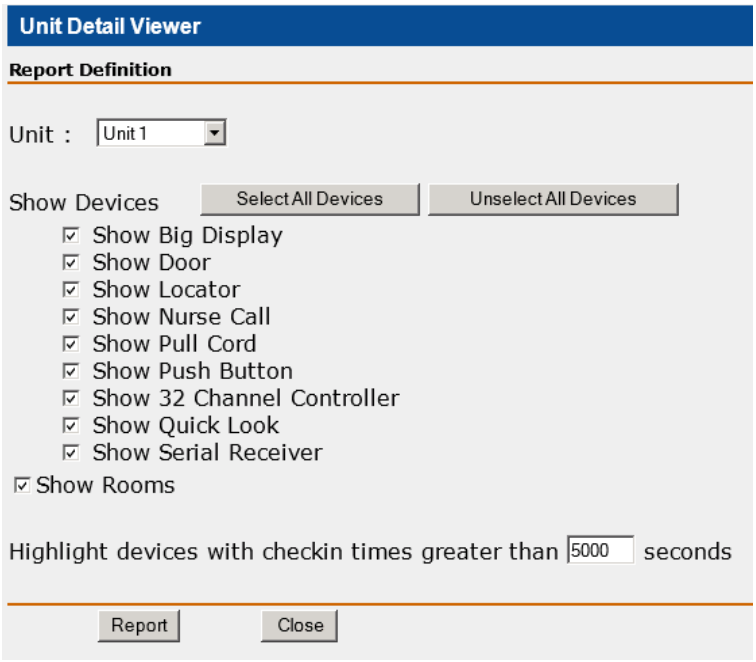
3. Enter a **Title** to name and save the report for future recall
4. Select a **Start** and **End** date that corresponds to the data to be retrieved and define **Attributes** that make up a specific report
5. Click **Report** to view the report

Unit Detail Viewer

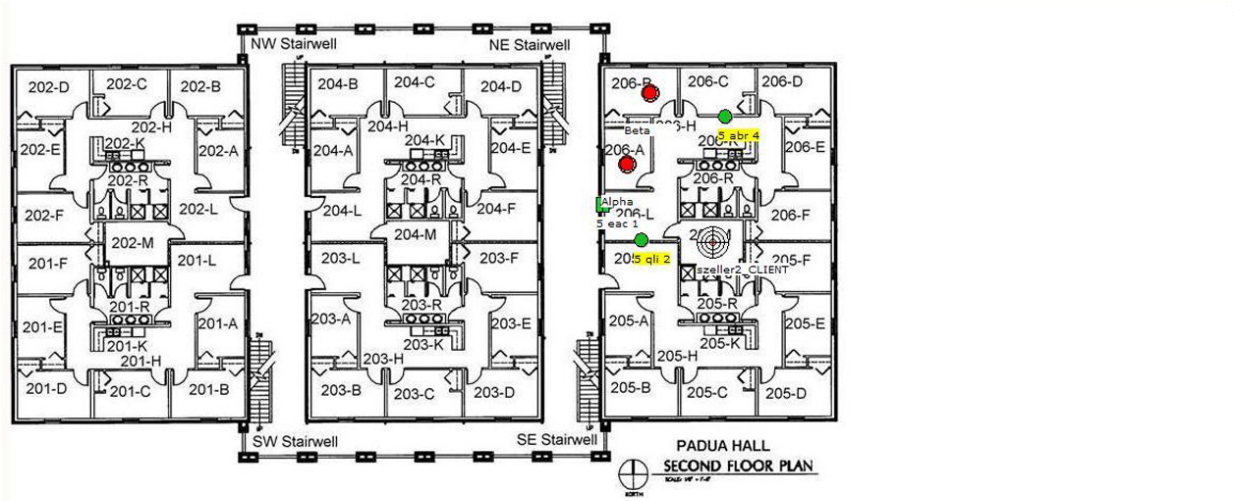
The Unit Detail Viewer option allows users to create Map Details Report of devices installed in the system.

To access the Unit Detail Viewer:

1. From the **Reports** home page, select **Unit Detail Viewer**
2. The **Unit Detail Viewer** Report Definition window opens
3. From the **Unit** pull-down, select a unit
4. The **Report Definition** window opens with a list of devices for that unit.



5. The **devices** available for display depends upon the devices assigned to the Unit.
6. Likewise, the **Show Rooms** and **Show Clients** checkboxes only appear if Rooms and Client systems are assigned to the Unit.
7. By default, all checkboxes are checked and the default value for **Highlight devices with checkin times greater than _____ seconds** is 5000.
8. Select the **Report** button to generate the following Unit Detail report.



Device	Type	SW Rev	Com	Chan	Addr	SuperTm	MaxTm*	Depth	Path
Door Man Rst CH19	doorwin	1.10	20		00:03:CD	Unit Default	841	0	Rout-0A31 CH19 > Door Man Rst CH19
Doorchk-03CE CH19	doorwin	1.20	20		00:03:CE	Unit Default	399	0	Rout-0A31 CH19 > Doorchk-03CE CH19
Emer-0381 CH19	pull	1.00	20		00:03:81	Unit Default	323	0	Rout-0A31 CH19 > Emer-0381 CH19
Rout-0A31 CH19	loc	1.03	20	19	00:0A:31	Unit Default	29	0	Rout-0A31 CH19
Rout-0A34 CH19	loc	1.06	20	19	00:0A:34	Unit Default	29	0	Rout-0A34 CH19
Pull-5229 CH19	pull	0.96	20		00:52:29	Unit Default	897	0	QLI-0E8B CH19 > Pull-5229 CH19
PCPull-0E3C CH19	pullp	0.96	20		00:0E:3C	Unit Default	1432	0	PCPull-0E3C CH19
SPullC-037B CH19	pullp	1.00	20		00:03:7B	Unit Default	1119	0	SPullC-037B CH19
SCPull-0397 CH19	pulls	0.96	20		00:03:97	Unit Default	607	0	QLI-0E8B CH19 > SCPull-0397 CH19
QLI-0E8B CH19	qli	1.09	20	19	00:0E:8B	Unit Default	29	0	QLI-0E8B CH19
Gate-0648 CH19	rxr	1.09	20	19	00:06:48	Unit Default	14	0	
Univ-4FC2 CH19	univ	0.16	19		00:4F:C2	Unit Default	1172	0	QLI-0E8B CH13 > Rout-0A1F CH13 > Univ-4FC2 CH19
Wall-0D82 CH19	wall	0.95	20		00:0D:82	180	132	0	QLI-0E8B CH19 > Wall-0D82 CH19

*MaxTime values shown as seen between 01/05/11 09:19 and 01/05/11 09:46

Return to Report Definition

9. Click **Return to Report Definition** to close the window and return to the Report Definition window

Chapter 3 – Software Configuration - Client

Introduction

This chapter provides details on Configuring the software for the client computers.

Client Properties

The Client Properties option allows you to set up which units are monitored from each client computer, configure the sound and display options for the computer, as well as define the map orientation when displayed on the computer.

To access the Client Properties page:

1. Select **Login** then select **Administrative Functions**
2. Select **Change Client Properties**
3. The Client Properties **Home** page opens

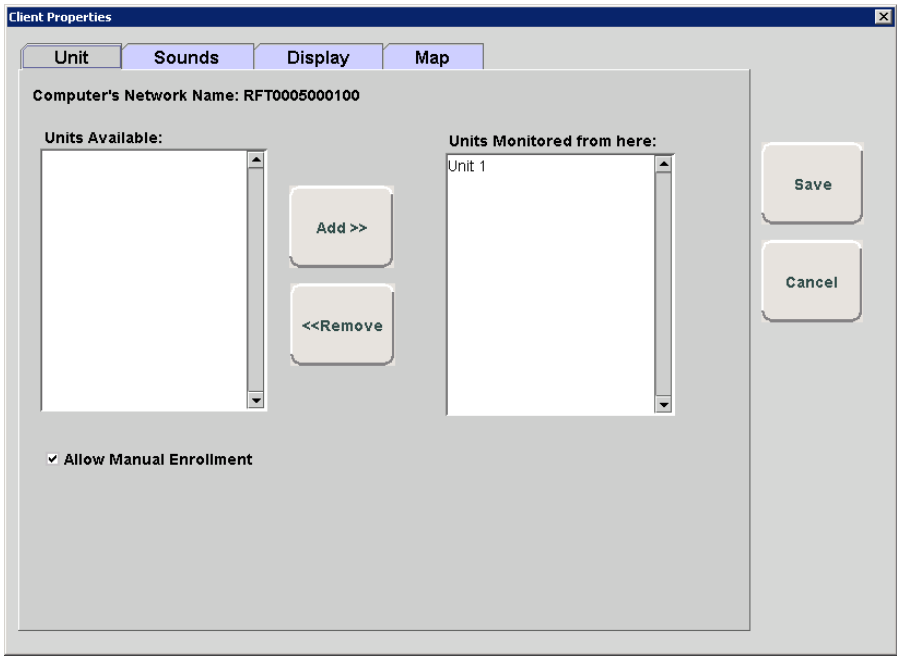
From the Client Properties home page, you can access the following:

- **Unit**: Allows you to add or remove units monitored at each client computer
- **Sounds:** Allows you to change the sound settings on the client computer
- **Display**: Allows you to change the display options like alarms, virtual keyboard, and tutorial help on the client computer
- **Map:** Allows you to change the map orientation displayed on the client computer

Unit

To add Units monitored at each client computer:

1. Go to the **Client Properties** window
2. Click the **Units** tab
3. On the Units tab, the name of the Client computer will appear next to **Computer's Network Name**



4. To add a unit to the list of those monitored at the Client computer's location, select it from the **Units Available** field
5. Click **Add>>** to move it to the **Units Monitored from here** field.
6. Click **Save** to save and return to the main window.

NOTE: Users cannot perform functions on a patient who is in a Unit that is NOT monitored by the Client computer they are using. You do NOT see alarms from transmitters or devices that are assigned to Units not monitored by the Client computer.

To remove Units monitored at each client computer:

1. To remove a Unit from the list of those monitored at the Client computer's location, select it from the **Units Monitored from here** field
2. Click **<<Remove** to move it to the **Units Available** field
3. Click **Save** to save and return to the main window

Manual Enrollment

To enable Manual Enrollment:

1. Go to the **Client Properties** window
2. Click the **Units** tab
3. Check **Allow Manual Enrollment** to enable this feature
4. Click **Save** to save and return to the main window

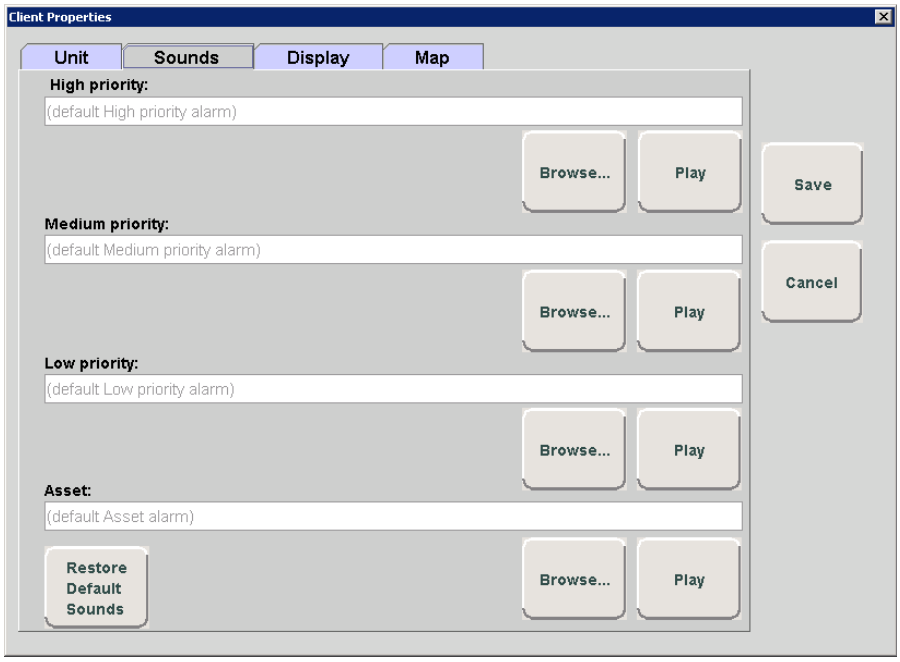
To disable Manual Enrollment:

1. Go to the **Client Properties** window
2. Click the **Units** tab
3. Uncheck **Allow Manual Enrollment** to disable this feature
4. Click **Save** to save and return to the main window.

Sounds

To change a client computer's Sound settings:

1. Go to the **Client Properties** window
2. Click the **Sounds** tab

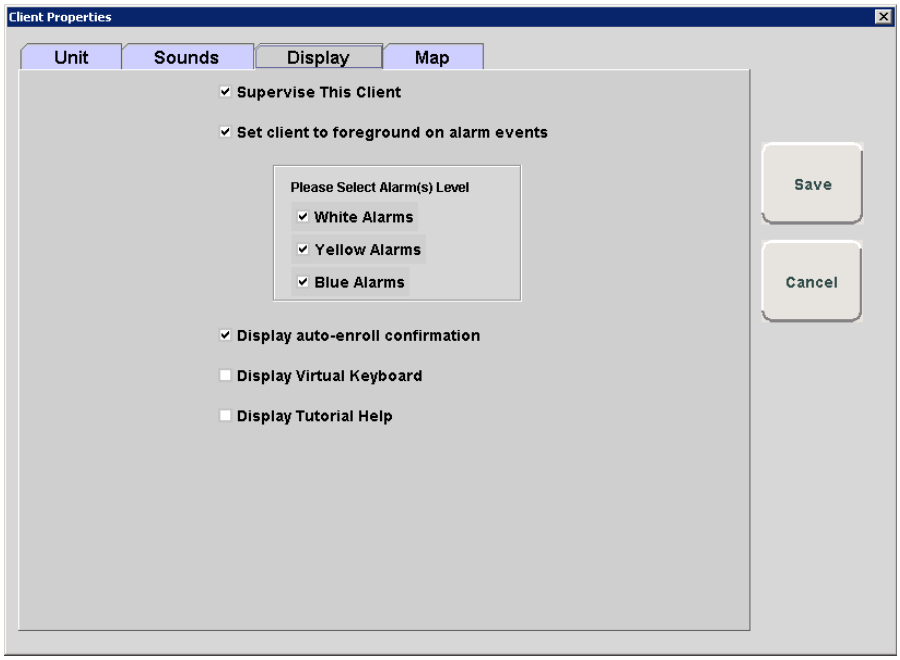


3. In each of the fields, click **Browse...** to select the location of the *.wav* file that contains the sound to be applied to the alarm
4. Click **Play** to hear a preview of the sound you selected
5. Click **Restore Default Sounds** if you wish to restore the default sounds
6. Click **Save** to save and return to the main window

Display

To change the Display Options on a client computer:

1. Go to the **Client Properties** window
2. Click the **Display** tab
3. Select the Client computer's display options that are relevant for your facility



- **Supervise This Client**: By default, this Client property is selected. Deselect this checkbox to allow users to restart the computer or perform a Microsoft session logoff without generating a Client Missing event.
- **Set client to foreground on alarm events**: This allows you to minimize/maximize the main application window. When an event occurs, the main window of the software is displayed as the active window, superseding the other application(s). A Red alarm event will always display the main window to the foreground. However, you can select lower priority alarms to display the main window to the foreground as well.

NOTE: If the client computer is running on a Windows 8.1 PC, the main application window is only brought to the foreground while the PC is in the Desktop mode. If the PC is displaying the Tile Interface, the main application windows is not brought to the foreground. Audible alarms will play in the background and outbound messages to pager, Quick Looks, etc. will be sent.

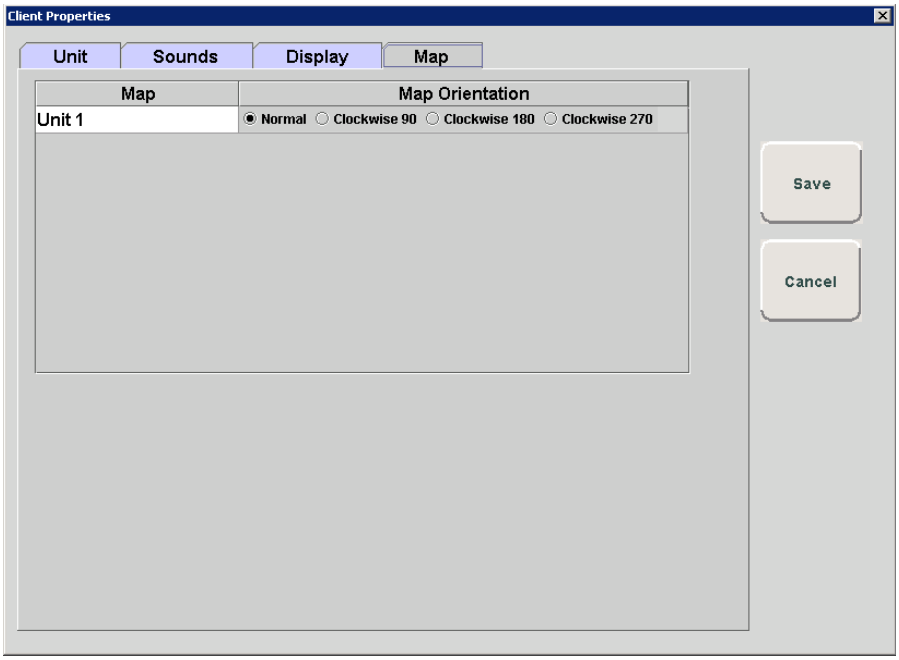
- **Display auto-enroll confirmation**: Select this checkbox if the Client computer is typically used to add infant information to the software database. When auto-enroll is selected as a system setting, a transmitter is automatically activated one minute after the banding material is connected. If this checkbox is selected, a white Auto-enroll event is displayed at the Client computer as soon as the transmitter is activated.

- **Display Virtual Keyboard**: Select this checkbox to display the touchscreen keyboard.
- **Display Tutorial Help**: Select this checkbox to display the Quick Reference Tutorial help screens. When enabled, the tutorial opens within the Event Information Window when responding to Red, Blue and White alarms. The tutorial contains a quick reference on how to respond to an alarm and common causes for the alarm.

Map

To rotate the Map Display on the client computer:

1. Go to the **Client Properties** window
2. Select the **Map** tab



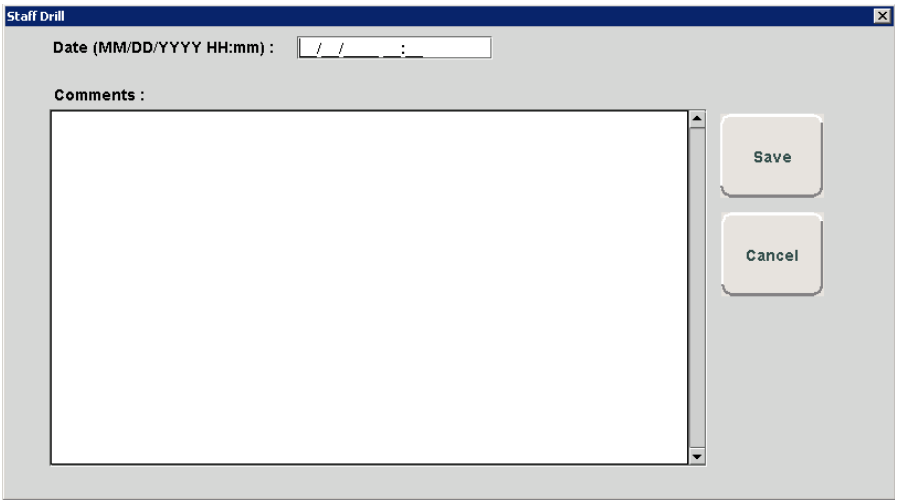
3. On the Map tab, identify the monitored Unit to which you want to rotate the map
4. Click the radio button next to the **Map Orientation** that you wish to be displayed for that unit
5. Click **Save** to save and return to the main window

Staff Drill

When a staff drill is requested, the attendant performing the drill enters the information in the Staff Drill window.

To access the Staff Drill window:

1. **Login** then select **Administrative Functions**
2. Select **Staff Drill**



3. Enter the **Date** of the Staff Drill as the two digit month, followed by the two digit day, followed by the four digit year. Enter the Time as the two digit hour followed by the two digit minute.

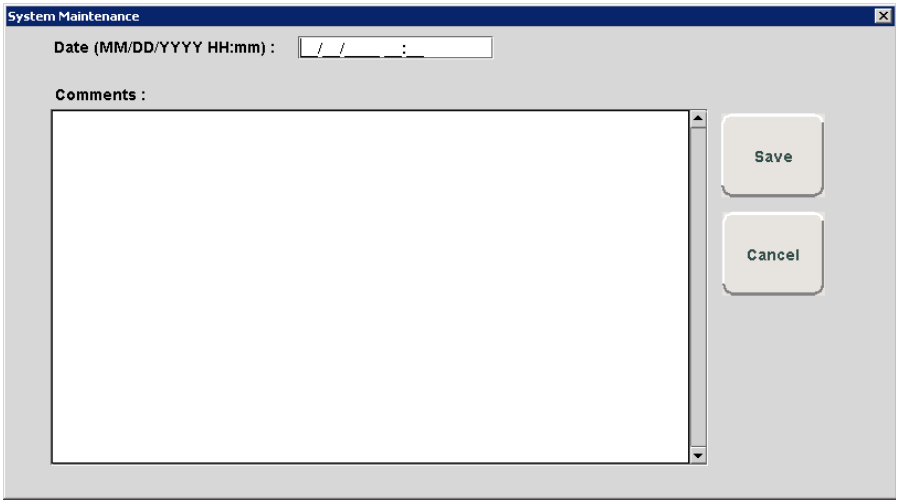
   The time must be entered in military format. Additionally, zeros must be used to fill in spaces that data is not entered in (i.e. 2:00 a.m. will be entered as 02:00 and 2:00 p.m. will be entered as 14:00).
4. In the **Comments** field, enter your comments
5. Click **Save** to save and return to the main window

System Maintenance

A log of maintenance performed on the system is logged in the System Maintenance window.

To access the System Maintenance window:

1. **Login** then select **Administrative Functions**
2. Select **System Maintenance**



3. Enter the **Date** of the System Maintenance as the two digit month, followed by the two digit day, followed by the four digit year. Enter the Time as the two digit hour followed by the two digit minute.

   The time must be entered in military format. Additionally, zeros must be used to fill in spaces that data is not entered in (i.e. 2:00 a.m. will be entered as 02:00 and 2:00 p.m. will be entered as 14:00).
4. In the **Comments** field, enter your comments
5. Click **Save** to save and return to the main window

Messaging

The software contains messaging functionality that enables the system to message system events and information to the facility staff via the standard pagers, email, Cisco phone, or text messaging.

NOTE: Smartphone pagers cannot receive system Schedule Messages, only Scheduled Events.

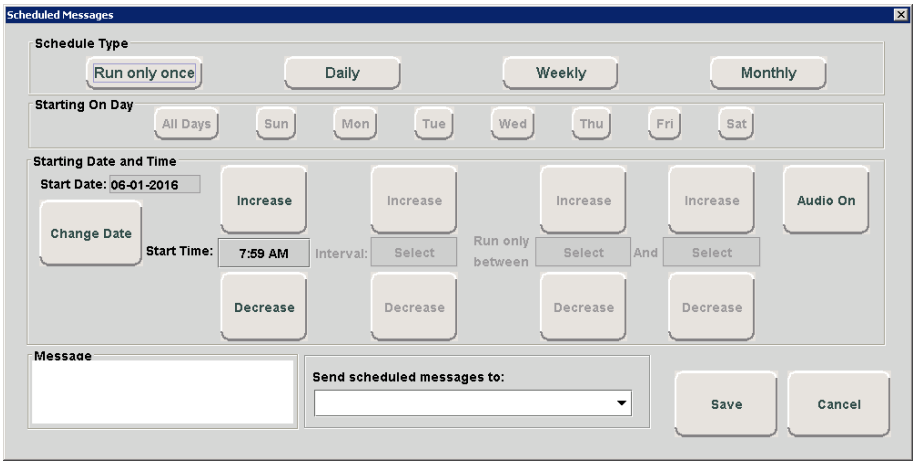
Schedule Messages

The Schedule Messages feature allows you to schedule system messages to be sent to staff one time only or on a daily, weekly or monthly basis.

NOTE: White Alarms are generated for patient level Scheduled Events. White Alarms are not generated for system level Scheduled Messages.

To add a Scheduled Message:

1. **Login** then select **Messaging Functions**
2. Select **Schedule Messages**
3. Click **Add** to open the Scheduled Messages window



4. Select the **Schedule Type** (Run only once, Daily, Weekly, or Monthly)
5. If you choose to run the scheduled message daily, you must select the day(s) you wish to run the message. Choose the day(s) from the **Starting On Day** field.

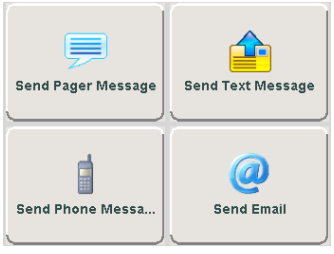
6. From the **Starting Date and Time** field, select a date and time to start the scheduled message. The current date is displayed in the Start Date field. To change the date, click on **Change Date** and choose a date from the popup calendar.
7. Choose a **Start Time**. The current time is displayed; click **Increase** or **Decrease** to select the desired start time.
8. If you choose to run the scheduled message more than once daily, you must select a run **Interval** and **Run only between times**. The Interval is how often you want the scheduled event to run. Increments are 1 minute (0:01) to 11 hours and 59 minutes (11:59).
9. Click **Increase** or **Decrease** to select the interval.
10. The **Run only between** range can be set for any minute of the day. Click **Increase** or **Decrease** to select the starting Run only between time AND click **Increase** or **Decrease** to select the ending Run only between time.

NOTE: The scheduled message Start Time must fall within the starting Run only between time and the ending Run only between time range. For example, a scheduled message with a start time of 8:00 A.M. must have a Run only between time window that includes 8:00 A.M. A Run only between time of 7:00 A.M to 10:00 A.M. is legitimate; it includes 8:00 A.M. A time of 4:00 A.M. to 7:00 A.M. is not a legitimate Run only between time.

NOTE: The scheduled message's Interval time must be less than the time window created by the Run only between times. For example, a scheduled message with an interval of 5 hours must have a Run only between time window of at least 6 hours.

11. The **Audio** button toggles On/Off. When Audio is turned On, the scheduled message will alarm at the Client computer(s)
12. Enter the message you wish to send in the free text **Message** field
13. From the **Send scheduled messages to** pull-down, select a message group or recipient to whom the message will be sent
14. Click **Save** to save your changes

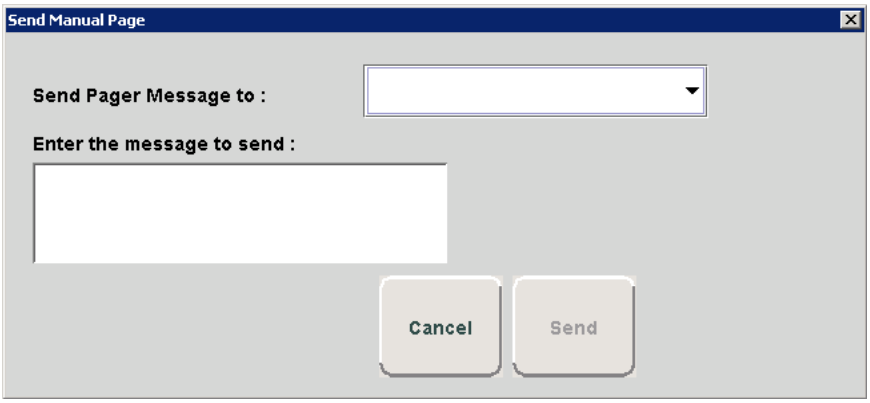
Send Message



In some cases, it may be necessary to send a manual message to a staff member. This feature can only be used if your system is configured for messaging. There are four messaging methods (pager, text, Cisco phone, and email). Select the method that best suit your needs. The example below is for sending a manual Pager Message.

To Send a manual Pager message:

1. **Login** then select **Messaging Functions**
2. Select **Send Pager Messages**



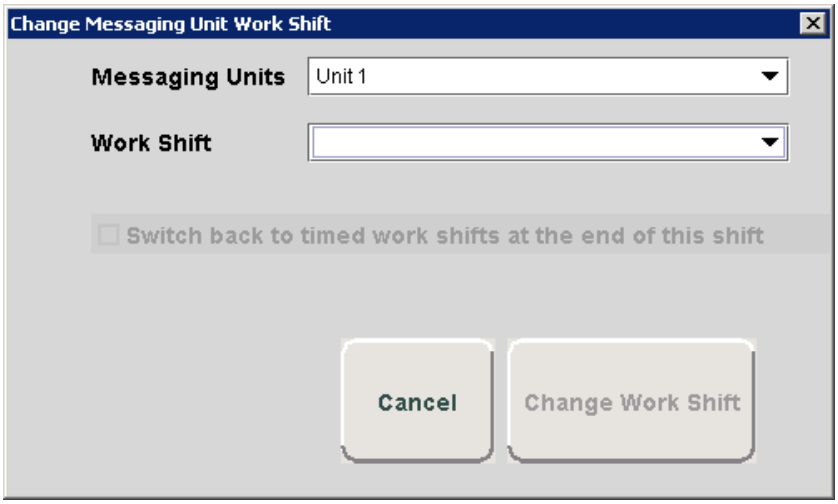
3. From the **Send Pager Message to** pull-down, select the pager or page group you wish to send a manual page to
4. Type your message in the **Enter the page message to send**: field
5. Click **Send** to send your message
6. Follow the same steps to send a text, email, or Cisco phone message

Messaging Unit Work Shift

In some cases, it may be necessary to change a page unit's work shift. Use this feature to select a different messaging unit and work shift. This feature can only be used if you currently use messaging shifts with your system.

To change a Messaging Unit Work Shift:

1. **Login** then select **Messaging Functions**
2. Select **Change Shift**



3. From the **Messaging Units** pull-down, select the Message Unit you wish to change
4. From the **Work Shift** pull-down, select a different work shift. The Change Work Shift button enables
5. If you wish to **switch back to timed work shift at the end of this shift**, click the checkbox.
6. Click the **Change Work Shift** button

This page intentionally left blank

Chapter 4 - Maintaining the System

Introduction

The 9450 Series, Quick Response Plus, Quick Response Premiere Wireless Call and 9500 Series Wired Call Systems should be commissioned at the point of installation by RF Technologies, Inc. However, in many cases the Radio Frequency (RF) environment of your facility can change. This can affect the performance of the system. This chapter is written primarily for facility or corporate maintenance employees who have a fundamental understanding of the system, basic electronics, electrical and mechanical aptitude. It is imperative that you read these directions in their entirety before beginning

CAUTION: Events occurring while the RFT JService is down will not be recorded. Alarming events will continue to generate and display in the software's Client application

NOTE: As each component of the system is specifically configured for your facility's particular needs, you may not have all of the options or features noted in this document.

Testing the System

It is the responsibility of the facility to establish and facilitate a regular maintenance schedule for your system, as outlined in the applicable system guides. This includes regular inspection, testing, and cleaning. RF Technologies, Inc. recommends monthly maintenance and testing of your system. It is also recommended that your facility keep records of maintenance and test completions.

WARNING: Failure to perform these tasks voids any or all product warranties.

Transmitters

Each 9450 transmitter has an expiration date printed on its side. The expiration date is based on the expected life of the battery inside the transmitter. The format used is EXP month/day/year.

You must check each transmitter's expiration date and remove any in use beyond their expiration date immediately. Test each transmitter by using the Transmitter Tester according to the directions in the applicable guides.

- Safe Place Transmitter User Guide (PN 0510-1121)
- Code Alert Transmitter User Guide (PN 0510-1122)
- Mother Transmitter User Guide (PN 0510-1020)
- Baby Check Transmitter User Guide (0510-1124)

You must test any new transmitters that are sent to your facility before using them by banding and bringing a transmitter within the detection zone of a monitored door to verify that the transmitter functions properly.

Additionally, it is important that you observe the low battery alarms from your transmitters. If a transmitter sends a low battery notification, you must remove that transmitter from use and replace it with a new transmitter, regardless of its expiration date.

Finally, examine the band (strap) used to attach the transmitter. You do not want the transmitter to be removed by someone other than an authorized staff member. Immediately replace any bands that are worn, torn, frayed or loose.

Exits

Each Exit system should be functionally tested and visually examined to verify that the system is working properly.

The 9450 Exit Alarm Controller is a rugged solid-state device and does not require regular maintenance or calibration, after correct installation, for proper operation. However, you must test the Exit Alarm Controller on a regular basis to verify correct operation. An active alarming band transmitter can be used to verify the functionality of each Exit Alarm Controller in the installation. RF Technologies, Inc. also makes dedicated Test Transmitters, in both 66kHz and 262kHz versions, available for this test purpose.

Each facility must test its complete system installation every month and keep records of test completion. Failure to test the system regularly can result in system failure and voids any or all product warranties.

NOTE: In the event that you test your system installation and it fails, immediately contact RF Technologies Inc. Technical Support at (800) 669-9946 or (262) 790-1771.

To test the Exits:

1. Go to each exit that is monitored by the system
   - Located on the Exit Alarm Controller are three colored lights, also known as LEDs (Light Emitting Diodes)
   - Verify that the red light labeled “Power” is on
   - There is a yellow signal light, which should be off
2. Approach the exit with a transmitter
   - Before you are within 4 ft. of the Exit Alarm Controller, the yellow signal light on the Controller must begin to flash or blink at a rate of about once per second.
   - If you have an electromagnetic lock (CodeLock™) on the door, the door must lock when a transmitter approaches
3. Open the door
   - The alarm must sound at the computer and you must hear beeping from the buzzer built into the Controller (if enabled)
   - If you have a Staff Alert Panel at the nurse’s station, an alarm must also sound at that location
   - If you have a CodeLock, you must verify that the door can be unlocked by activating the delayed egress feature. For more

information, see the CodeLock Electromagnetic Door Lock Installation Guide (PN 0510-1002)

4. Close the door
5. Reset the alarm by pressing the 4-digit security code
   - The default code is 1-3-7-9; the current selected code must be used. The green status light will flash on for 1 second.
6. Repeat the test several times
7. In the case of a double door, confirm that the system issues an alarm when either door is opened
8. Verify that the keypad buttons are working properly
9. If the system at your facility has a bypass code, verify that it is working properly
   - Enter the bypass code
   - The green status light comes on and stays lit for a period of time configured in your system setup
   - While the green light is on, open the door with a transmitter in the vicinity. An alarm will not sound
   - Close the door
   - If you have anti-tailgate enabled, the system will immediately re-arm (indicated by the green light turning off)
   - Open the door again to verify that it alarms properly
10. If any of the testing steps above fail, contact RF Technologies Inc. Technical Support at (800) 669-9946 or (262) 790-1771

CodeLock™

To test the CodeLocks (reference the applicable CodeLock Manual):

- CodeLock Electromagnetic Door Lock Installation Guide (PN 0510-1002)
- CodeLock 600lb Electromagnetic Door Lock Installation Guide (PN 0510-1038)
- 1500 Lb. Electromagnetic Door Lock Installation Guide (PN 0510-1039)

Visual System Inspection

After you test the exits, it is important to make sure that all of the components of the system are installed correctly and not physically damaged. Visually inspect the following components:

- Exit Alarm Controller
- Raceway
- Exit Alarm Receivers
- Reed Switches
- CodeLocks

Exit Alarm Controller

Verify that the Exit Alarm Controller is installed correctly and is not physically damaged:

- The enclosure must not be damaged, and must be mounted tight to the wall
- The screws holding the faceplate of the unit must be tight
- The lights on the controller must not be pushed in or damaged
- The keypad buttons must not be worn or marked where a person could guess the reset code
- The Touchpad Exit Controller keypad lights up when touched/activated

Raceway

Verify that the Raceway is installed correctly and is not physically damaged:

- If your system is surface mounted, the plastic raceway (sometimes referred to as Wiremold® or Panduit®) should be examined
- It should not be cracked, open, or pulled loose from the wall
- Fittings or couplings should be present at all corners and splicedso that the wiring is not visible
- Repair or replace damaged raceway
- Raceway can be painted with a latex paint to match the walls

Exit Alarm Receiver

Verify that the Exit Alarm Receiver is installed correctly and is not physically damaged:

- There should be two receivers installed per single door, or four per double door
- Verify that the receivers are mounted tight to the wall
- It must not be cracked, open, or pulled loose from the wall

Reed Switch

The reed switches are located on the door and door frame. They let the system know when the door is open or closed. There are two parts: the switch (on the frame) and the magnet (on the door).

Verify that the Reed Switches are installed correctly and are not physically damaged:

- The system reed switches are brown in color with “Code Alert” printed in gold foil lettering on the front of them
- When the door is closed, the two parts of the reed switch must be next to each other (within ½”). There must be a minimum 1/16th to 1/8th inch gap between the two parts when the door is closed. They should not strike each other when the door slams.
- Examine the door’s closer(s), latch(es), and hinges. Make sure that the door closes properly. The door must not drag or not close and must latch completely. Repair the door if necessary. If the reed switch senses the door is open because it does not close completely, the system will alarm when an alarming band transmitter is in the vicinity.

CodeLock

Verify that the CodeLock Electromagnetic Locks connected to the system are installed correctly and are not physically damaged:

- Read the CodeLock Electromagnetic Door Lock Installation Guide (PN 0510-1002) in its entirety before beginning
- The functionality of CodeLock is regulated by local and state codes which vary by municipality. Contact your local Fire Inspector (or the authority having jurisdiction) if you have any questions. Most states have adopted a version of NFPA 101-16 5-2.1.6 Special Locking Arrangements. A reprint of the NFPA requirements is located in the back of the CodeLock Electromagnetic Door Lock Installation Guide (PN 0510-1002)
- Visually inspect the CodeLocks by verifying that:
  - There are not any loose or visible wires
  - The door closes, latches and locks properly
  - The armature plate has room to move according to the CodeLock Electromagnetic Door Lock Installation Guide (PN 0510-1002)

Adjusting Antenna

If you have construction in the area or changes are made in the duct work above the ceiling in your facility, the RF signature changes. Move the applicable ABR's antenna to a quiet zone in the facility to avoid RF noise.

Contact RF Technologies Technical Support at (800) 669-9946 or (262) 790-1771 before moving any antenna.

For more information, see the UHF Antenna Installation Guide (PN 0510-1009).

Reviewing Alarm Reports

You must review the alarm reports for your system in order to assess the overall system functionality. Failure to review the alarm reports can result in system failure and can void any or all product warranties. A significant number of false alarms could be an indicator of inadequate training, environmental RF noise, or system coverage issues.

If you have questions or concerns about persistent issues, contact RF Technologies, Inc. Technical Support at (800) 669-9946 or (262) 790-1771.

For more information about using reports, see the following guides:

- Infant Security System Software User Guide (PN 0510-0078)
- Wanderer Monitoring System Software User Guide (PN 0510-1017)
- Patient Monitor System Software User Guide (PN 0510-1030)

Staff Assessment

You must periodically assess staff response to alarms in accordance with your facility's total security plan. For example, planning mock patient elopement, or mock patient abduction drills, etc.

In addition, regular refresher training should be provided for the staff. For assistance, contact RF Technologies. Inc. Technical Support at (800) 669-9946 or (262) 790-1771.

Database Maintenance

Technicians, installers and users are responsible for archiving the configuration database, for both new and existing systems. RF Technologies, Inc. recommends archiving monthly or whenever a change is made to the following configurations: Devices, Units, Rooms and Users. See *Database Archive and Backup – Series 10.x Software* (PN 0510-05275) for additional details.

Archive Data

1. The configuration database is archived via the Series 10.x Software
2. The Archive function archives all configuration data except data for patients and transmitters since patients and transmitters are admitted and discharged on a regular basis
3. The SQL database (history of events) is automatically purged and archived monthly

Restore Data

An archived configuration is stored in a folder with the archived date and time such as *db.2008-08-06-09-21-02*. The date and time are in the format: YYYY-MM-DD-hh-mm-ss. The path to this folder is **C:\Program Files (x86)\RF Technologies\db**. Folders are stored chronologically, according to the archived date.

To restore Archived Data:

1. To restore the archived data to a second computer, follow the path to the db folder and copy it onto a removable media such as a USB drive.
2. Copy the db folder from the USB drive to the db folder on the second computer, following the same path.
3. You can now go to **Configuration>>Maintenance>>Archive** and restore the configuration to the second computer.

NOTE: Backups should be kept in a secure location off of the Central Server.

Replace a Repeater

To Replace a Repeater:

1. Determine the ID number of the Repeater that is being replaced, *idold*
2. Determine the ID number of the replacement Repeater, *idnew*
3. Add the replacement Repeater to the Quick Response Plus Device ID List
4. Replace the Repeater hardware
5. Ensure that the Repeater is on the correct network for the Network Coordinator
6. Assign the new Repeater to the same unit as the old Repeater, if the old Repeater was assigned to a unit
7. Remove the old Repeater from the Quick Response Plus Device ID List
8. Open a Command Prompt window and **Run as administrator**
9. Click the **Start** button
10. Click the magnifying glass icon
11. Type *command*
12. Right click **Command Prompt**
13. Select **Run as administrator**
14. If the prompt does not start with "C:", type "*C:*" and press **Enter**
15. Type the following command "cd *C:\Program Files (x86)\RF Technologies\sql*"
16. Type the following command "*ChangeSurveyedRepeaterID.bat idold idnew*", replacing idold with the device ID of the replaced Repeater, and idnew with the device ID of the replacement Repeater
17. Restart the Server

This page intentionally left blank

Appendix A – User Type Permissions

Introduction

Functions/permissions allowed to the user can be quickly assigned by selecting a User Type with those functions already setup or you can manually assign user functions. The default system User Types are as follows:

Code Alert

	Admin	Caregiver	Nurse	Secretary	Staff	Super User
Adjust	X	X	X		X	X
Admit	X	X	X	X	X	X
Archive Viewer	X					
Change Paging Shift	X					X
Clear	X	X	X	X	X	X
Close Software	X					
Configure Clients	X					
Configure Database	X					
Configure Pager	X					X
Configure System	X					X
Configure Users	X					X
Discharge	X	X	X	X	X	X
Escort	X	X	X		X	X
Maintenance	X					X
Monitor Help	X	X	X			X
Protect By Login	X					
Send Page	X	X	X		X	X
Silence	X	X	X	X	X	X
Staff Drill	X					X
Transfer	X	X	X		X	X

Safe Place

	Admin	Biomed	Caregiver	Health Unit Coord	Nurse	Secretary	Security	Staff	Super User
Adjust	X		X	X	X			X	X
Admit	X		X	X	X	X		X	X
Archive Viewer	X	X							
Change Paging Shift	X								X
Clear	X		X	X	X	X	X	X	X
Close Software	X						X		
Configure Clients	X	X							
Configure Database	X	X							
Configure Pager	X	X							X
Configure System	X	X							X
Configure Users	X								X
Discharge	X		X	X	X	X		X	X
Escort	X		X	X	X			X	X
Maintenance	X	X			X				X
Monitor Help	X		X	X	X				X
Pre-Enroll	X		X	X	X			X	X
Protect By Login	X								
Receive High Risk Admit Emails	X						X		
Send Page	X		X	X	X			X	X
Silence	X		X	X	X	X	X	X	X
Staff Drill	X								X
Transfer	X		X	X	X			X	X

Appendix B – Code Alert System Defaults

Introduction

The default system configuration settings for the Code Alert system are as follows:

To access the System Settings:

1. Login then select **Administrative Functions**
2. Select **Configuration**
3. Select **Configuration** then select **Settings**

Section	Option	Default Setting
Settings - Global		
Facility	Name, Address, Phone	Customer defined
General	HIPAA Options	No HIPAA Filtering
	Show Date and Time on QuickLook	Checked
	Hide Workstation Map Device Icons	Not checked
	Confirm Discharge	Not checked
	Confirm Escort	Not checked
	Confirm Transfer	Not checked
	UL-1069 / UL-2560 Low Battery Alarm Notification	Not checked
	Hide Event Time in Client Lists	Not checked
	Alarm Volume Level	100%
	Alarm Silence Timeout After	5 minutes
	Auto Close Software	1 minute
	Inactive User Log Off	1 minute
	Timed Event Warning Time	15 minutes
	Workstation Default Screen	Map
	Device Fault / Low Battery Alarm Silence Period	24 hours
	Workstation Census View Column Order	Name Room Status Location Destination Time Remaining Transmitter ID Risk Gender

Section	Option	Default Setting
9450	Auto-Enroll Transmitters	Checked
	Alarm Transmitters Which Are Not Auto-Enrolled	Checked
	Require Multiple ABRs	Not checked
	Confirm Admit	Not checked
	Confirm Adjust	Not checked
	TroubleShooter Enabled	Not checked
	Enable Global Clear of Auto-Enroll Confirmations	Not checked
	Lockdown on Cut Band Alarms	All Exits
	Lockdown on Band Off Alarms	All Exits
	Minimum Checkins Required	3
	Transmitter Pre-Enroll Duration	Not available in Code Alert
Quick Response Plus	Use Location Engine for Pendant Alarms	Not checked
	Use Location Engine for Fall Alarms	Not checked
Authentication	Enable LDAP Authentication	Not checked
	LDAP Server Hostname	Customer defined
	Domain Name	Customer defined
	Authentication Cache Expiry	2 minutes
	Login Requires	Card & Password Only
	Port Number	389
	Maximum Invalid Logins	3
	Bind Method	Negotiate
	Enable Kerberos	Checked
Email	SMTP Server Address	Customer defined
	User (from address)	Customer defined
	Password	Customer defined
	Send High Risk Admit Email	Not checked
Escort Destinations	Enable Mom-Baby Time Tracking on Escort Destinations	Not checked
Settings - Units		
Times	Device Supervise Time	2 hours
	Transmitter Supervise Time	24 hours
	Discharge Time	5 minutes
	Adjust Time	5 minutes
	Band slippage check	0
	Enforce the Joint Commission Reporting	Not checked

Section	Option	Default Setting
Smart Sense	Smart Sense Enabled	Not checked
	Capacitance	1 minute
	Resistance	No Delay
	Check Band Warning Only	Not checked
	Escalate Check Band to Band Off Alarm after	Checked 5 minutes
	Immediate Band Off	Not checked
	Display Check Bands on Quick Look Displays	Checked
Wander Management	Enable Loiter Notifications	Checked
	Loiter Delay Time	5 minutes
	Display Door Alarm at start of egress cycle	Checked
Edit Map Options	Show Devices	Checked
	Show Rooms	Checked
	Show Clients	Checked

This page intentionally left blank

Appendix C – Safe Place System Defaults

Introduction

The default system configuration settings for the Safe Place system are as follows:

To access the System Settings:

1. Login then select **Administrative Functions**
2. Select **Configuration**
3. Select **Configuration** then select **Settings**

Section	Option	Default Setting
Settings - Global		
Facility	Name, Address, Phone	Customer defined
General	HIPAA Options	Show Room Number Only
	Show Date and Time on QuickLook	Checked
	Hide Workstation Map Device Icons	Not checked
	Confirm Discharge	Not checked
	Confirm Escort	Not checked
	Confirm Transfer	Not checked
	UL-1069 / UL-2560 Low Battery Alarm Notification	Not checked
	Hide Event Time in Client Lists	Not available in Safe Place
	Alarm Volume Level	100%
	Alarm Silence Timeout After	5 minutes
	Auto Close Software	1 minute
	Inactive User Log Off	1 minute
	Timed Event Warning Time	15 minutes
	Workstation Default Screen	Census
	Device Fault / Low Battery Alarm Silence Period	24 hours
	Workstation Census View Column Order	Room Name Gender Location Status Destination Time Remaining Transmitter ID Risk

Section	Option	Default Setting
9450	Auto-Enroll Transmitters	Checked
	Alarm Transmitters Which Are Not Auto-Enrolled	Not checked
	Require Multiple ABRs	Checked
	Confirm Admit	Not checked
	Confirm Adjust	Not checked
	TroubleShooter Enabled	Not checked
	Enable Global Clear of Auto-Enroll Confirmations	Not checked
	Lockdown on Cut Band Alarms	All Exits
	Lockdown on Band Off Alarms	All Exits
	Minimum Checkins Required	3
	Transmitter Pre-Enroll Duration	12 hours
Authentication	Enable LDAP Authentication	Not checked
	LDAP Server Hostname	Customer defined
	Domain Name	Customer defined
	Authentication Cache Expiry	2 minutes
	Login Requires	Card & Password Only
	Port Number	389
	Maximum Invalid Logins	3
	Bind Method	Negotiate
	Enable Kerberos	Checked
Email	SMTP Server Address	Customer defined
	User (from address)	Customer defined
	Password	Customer defined
	Send High Risk Admit Email	Not checked
Escort Destinations	Enable Mom-Baby Time Tracking on Escort Destinations	Not checked
Settings - Units		
Times	Device Supervise Time	System Default
	Transmitter Supervise Time	5 minutes
	Discharge Time	5 minutes
	Adjust Time	5 minutes
	Band slippage check	0
	Enforce the Joint Commission Reporting	Checked

Section	Option	Default Setting
Smart Sense	Smart Sense Enabled	Checked for new units
	Capacitance	1 minute
	Resistance	No Delay
	Check Band Warning Only	Not checked
	Escalate Check Band to Band Off Alarm after	Checked 5 minutes
	Immediate Band Off	Not checked
	Display Check Bands on Quick Look Displays	Checked
Wander Management	Enable Loiter Notifications	Checked for new units
	Loiter Delay Time	5 minutes
	Display Door Alarm at start of egress cycle	Checked for new units
Edit Map Options	Show Devices	Checked
	Show Rooms	Checked
	Show Clients	Checked

This page intentionally left blank

Appendix D – Client Configuration Defaults

Introduction

The default system configuration settings for the client computers are as follows:

To access the System Settings:

1. Login then select **Administrative Functions**
2. Select **Change Client Properties**

Section	Option	Default Setting
Unit		
	Units Available	Customer defined
	Units Monitored from here	Customer defined
	Allow Manual Enrollment	Not checked
	Enable Kerberos	Not checked
Sounds		
	High Priority	(default High priority alarm)
	Medium Priority	(default Medium priority alarm)
	Low Priority	(default Low priority alarm)
	Asset	(default Asset alarm)
Display		
	Supervise This Client	Checked
	Set client to foreground on alarm events	Checked
	Select Alarm(s) Level	White Alarms Yellow Alarms Blue Alarms
	Display auto-enroll confirmation	Not checked
	Display Virtual Keypad	Not checked
	Display Tutorial Help	Not checked
Map		
	Map Orientation	Normal

This page intentionally left blank

Revision History

Revision	Change
A	Release
B	Updated for release 10.1
C	Updated for release 10.2
D	Updated for release 10.3 **Added**: Appendix A (Default User Type Permissions)
E	**Updated**: Configuration sections to clearly call out default settings **Added**: Appendix B for Code Alert default settings **Added**: Appendix C for Safe Place default settings **Added**: Appendix D for Client Configuration default settings
F	**Updated:** Adding a User section to clarify password rules when utilizing LDAP authentication
G	**Updated:** Default settings in Appendix B (Transmitter Pre-Enroll is not available for Code Alert, LDAP Port number is pre-populated with 389, and LDAP Enable Kerberos is checked on by default) **Updated:** Default settings in Appendix C (Hide Event Time in Client Lists and QR Plus is not available for Safe Place, LDAP Port number is pre-populated with 389, LDAP Enable Kerberos is checked on by default, Transmitter Supervise Time is 5 minutes, and Smart Sense Enabled, Display Door Alarm at start of Egress and Enable Loiter Notifications are checked on by default for new units) **Updated:** System overview maps

3125 North 126th Street, Brookfield, WI 53005
Phone 800.669.9946 fax 262.790.1784
www.rft.com

0510-1129-G
Release Date: 09/2018

RFTWI rftsafety RF Technologies

Made in USA