





Table of Contents

1.0	Introduction	6
1.1	How to Use This Guide	7
1.2	Compatible Browsers	8
1.3	Contact Us	8
2.0	MiCare Central Software Installation	9
2.1	Requirements	
2.2	Before Installing	
2.3	Installing	11
3.0	Logging in to the Admin Portal	12
3.1	Logging in to the Admin Portal	13
3.2	Managing Administrators	13
4.0	Configuring Your Campus	16
4.1	Campus	17
4.2	Entering Your Campus Information	17
4.3	Managing Buildings	17
4.4	Managing Wings	
4.5	Managing Floors	20
4.6	Managing Rooms	21
5.0	Managing Attendants	24
5.1	Attendants	25
5.2	Adding an Attendant	25
5.3	Editing an Attendant	25
5.4	Changing the PIN for an Attendant	25
5.5	Deleting an Attendant	26
6.0	Managing Residents	27
6.1	Residents	28
6.2	Adding a Resident	28
6.3	Adding Medication Reminders for a Resident	29
6.4	Adding Family Contacts for a Resident	29
6.5	Adding Medical Contacts for a Resident	29
6.6	Editing Resident Information	30
6.7	Deleting a Resident	30



7.0	Editing Global Device Templates	31
7.1	Coordinators, Routers, and End Devices	32
7.2	Global Device Templates	32
7.3	NC-2000 Patient Unit Global Template Settings	32
7.4	NC-210 Beacon Global Template Settings	38
7.5	NC-103 Pull Station Global Template Settings	39
7.6	NC-220 ZF3 Global Template Settings	40
7.7	NC-500 Pendant Global Template Settings	41
8.0	Managing Devices	43
8.1	Devices	44
8.2	Adding a Device	44
8.3	Assigning a Device	46
8.4	Assigning an Ultrasonic ID to Patient Units and Beacons	46
8.5	Retrieving the Patient Unit's Log File	46
8.6	Editing a Device	47
8.7	Deleting a Device	47
9.0	Creating Groups	48
9.1	Creating a Group	49
9.2	Editing a Group	49
9.3	Deleting a Group	50
10.0	Defining Rules	51
10.1	Rules	52
10.2	Event	52
10.3	Escalations	57
10.4	Output Scenario	57
10.5	Target	61
10.6	Response	61
10.7	Creating a Rule	61
10.8	Editing a Rule	62
10.9	Disabling and Enabling a Rule	62
10.10	Deleting an Escalation	62
10.11	Deleting a Rule	63
11.0	Running Reports	64
11.1	Reports	65
11.2	Monitoring Facility Call Point Performance	
11.3	Monitoring Nurse Service Time	66
11.4	Generating Device Maintenance Reports	67



11.5	Generating Resident Medication Reports	67
11.6	Generating Detailed Archived Alerts Reports	67
11.7	Generating Summarized Archived Alerts Reports	68
11.8	The Report Window	69
12.0	Archived Alerts	70
13.0	Network View	71
13.1	Network View	72
13.2	Devices	72
14.0	The MiCare Processor	73
14.1	Accessing the MiCare Processor	74
14.2	Output Listing	74
14.3	Notification Testing	75
14.4	Settings	75
14.5	Debug	76
14.6	Monitoring	77
15.0	Warranty and Warning Information	78



1.0 Introduction

This guide describes how to configure your facility through the Admin Portal in the MiCare Central Station (Central). Use Central to set up your facility, add the system users, and configure the MiCare devices.

This chapter covers the following topics:

- How to Use This Guide
- Setting Up Your Campus



1.1 How to Use This Guide

This guide explains how to configure a Mircom MiCare Nurse Call System installation. Configuration is done by the administrators of the Nurse Call System, and not by the users (that is, attendants) of the Nurse Call System. For information on using the Nurse Call System, see LT-2076, the MiCare Nurse Call System User's Guide.

Configuring a Nurse Call System involves the following steps:

- Setting Up Your Campus
- Entering Attendants and Residents
- Setting Up Devices
- Setting Up Groups
- Defining Device Rules
- Maintaining the Nurse Call System

Sections 1.1.1 to 1.1.6 give a brief introduction to each of these steps as well as where to find detailed information on them.

Section has contact information for Mircom customer and technical support.

1.1.1 Setting Up Your Campus

In a typical installation, the setup procedure for your campus is the following:

1. Install the MiCare Nurse Call System devices.

The MiCare devices for your site should already be installed and operating before you enter them into Central. You should also have a device installation table with the MAC addresses, device types, and location for each device.

Information on how to install the Nurse Call System devices can be found in LT-2074, the MiCare Nurse Call System Installation Manual.

2. Configure your site.

This involves creating accounts for the administrators and setting up your campus with buildings, floors, and rooms. Information on these tasks can be found in the following chapters:

- Chapter 3.0, Logging in to the Admin Portal, on page 12.
- Chapter 4.0, Configuring Your Campus, on page 16.

1.1.2 Entering Attendants and Residents

Attendants and residents should be entered next so that you can assign MiCare devices to them, include them in groups, and create rules for them. Information on adding attendants and residents can be found in the following chapters:

- Chapter 5.0, Managing Attendants, on page 24.
- Chapter 6.0, Managing Residents, on page 27.



1.1.3 Setting Up Devices

Device setup involves configuring and then adding devices to your site. Before you add devices to Central, you must edit the global device templates for each device. Information on editing global device templates and on adding devices can be found in the following chapters:

- Chapter 7.0, Editing Global Device Templates, on page 31.
- Chapter 8.0, Managing Devices, on page 43.

1.1.4 Setting Up Groups

You can group attendants, devices and residents. Groups are convenient when you need to notify more than one entity through Central. Information on creating groups can be found in the following chapter:

• Chapter 9.0, Creating Groups, on page 48.

1.1.5 Defining Device Rules

The MiCare Nurse Call System is driven by rules. Rules define what actions the Nurse Call System takes when events happen on MiCare devices. Information on creating rules can be found in the following chapter:

Chapter 10.0, Defining Rules, on page 51.

1.1.6 Maintaining the Nurse Call System

Built into the Nurse Call System are tools to monitor the performance of the system. You can run reports to see how the facility is performing or to create a daily task lists. The MiCare processor can be used to troubleshoot communication problems between the devices and the Central server. Information on running reports and on MiCare Processor can be found in the following chapters:

- Chapter 11.0, Running Reports, on page 64.
- Chapter 14.0, The MiCare Processor, on page 73.

1.2 Compatible Browsers

The Admin Portal works best with Firefox.

1.3 Contact Us

1.3.1 Canada and USA

Toll Free: 1-888-660-4655

Local: 905-660-4655

Fax: 905-660-4113

1.3.2 Website

http://www.mircom.com



2.0 MiCare Central Software Installation

This document describes how to install the MiCare Central Software.

This chapter covers the following topics:

- Requirements
- Before Installing
- Installing



2.1 Requirements

- Windows Server 2012 R2, Windows Server 2008 R2, or Windows 10
- 1.4 GHz 64-bit processor minimum
- 512 MB RAM minimum
- 2 GB disk space minimum
- Internet access

ĺ

Note: This installer:

- installs a new version of the MiCare Central Software,
- upgrades the MiCare Central Software from version 1.1.1 to the latest version.

2.2 Before Installing

If you are upgrading from MiCare Central Software version 1.1.1 or 1.1.2, follow these instructions before installing.

- 1. Open Internet Information Services (IIS) Manager.
- 2. In Internet Information Services (IIS) Manager, right-click the MiCare website, then select **Remove**.

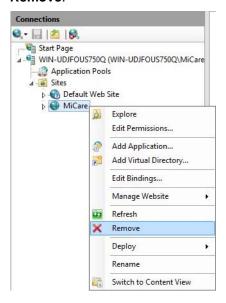


Figure 1 Internet Information Services (IIS) Manager

3. Go to section 2.3.



2.3 Installing

- 1. Double-click the file **MiCare Installer v.x** to start the installation.
- 2. Follow instructions on the screen.
- 3. On the Email Server Configuration window, enter your own email server information, or leave the information as is. Consult your network administrator for assistance.

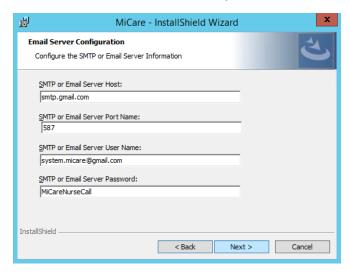


Figure 2 Email Server Configuration

4. On the Database Server window, click Next.

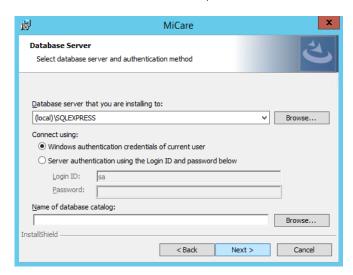


Figure 3 Database Server

5. Follow the instructions on the screen to complete the installation.



3.0 Logging in to the Admin Portal

Configuration of the MiCare system is done through the Admin Portal in Central. You must log in to the Admin Portal as an administrator before you can perform tasks such as adding users, configuring your site, configuring devices, and more.

The following topics are covered in this chapter:

- Logging in to the Admin Portal
- Managing Administrators



3.1 Logging in to the Admin Portal

Configuration for the MiCare Nurse Call System is done through a web interface to the MiCare Central Station (Central).

To log in to the Admin Portal:

- 1. Open your browser and enter the URL for the MiCare Central server in the address field.
- 2. From Central, click Admin Portal.
- 3. In the User ID box, type your user name. The default user name is admin.
- In the Password box, type your password. The default password is password1.
- 5. Click Login.

If you are a new user, you will be prompted to provide a security question, a security answer, and a new password. After typing in this information, click **Change Password** to access the Admin Portal.



Figure 4 Change Password

The security question and answer are stored in the MiCare system and are used to authenticate you when you request a password change.

After logging in, you are taken to the Admin Portal. All tasks related to the administration of the MiCare system are performed in the Admin Portal.

3.2 Managing Administrators

Administrators have complete access to the MiCare system, including the ability to manage other administrators. The following tasks are covered in this section.

Adding Administrator Accounts



- · Editing Administrator Accounts
- Resetting an Administrator Password
- Deleting Administrator Accounts

3.2.1 Adding Administrator Accounts

You can add administrator accounts as needed. All administrators have the same rights and permissions on the MiCare system.

To add a new administrator:

- 1. Log in to the Admin Portal.
- 2. Click Administrators.
- 3. Click Add New Administrator.
- 4. Type in the information for the new administrator. Fields with a red asterisk are required.
- 5. Click Save Administrator.

3.2.2 Editing Administrator Accounts

You can update the information for an administrator when necessary.

To update the information for an administrator:

- 1. Log in to the Admin Portal.
- 2. Click Administrators.
- 3. Find the administrator in the **Administrators** table, and then click **Edit** for that administrator.
- 4. Make your changes to the administrator information.
- 5. Click Save Administrator.

3.2.3 Resetting an Administrator Password

To reset the password for an administrator:

- 1. Log in to the Admin Portal.
- 2. Click Administrators.
- 3. Find the administrator in the **Administrators** table, and then click **Edit** for that administrator.
- 4. Type in the new password in the **Temporary Password** and **Confirm Password** fields.
- 5. Click Reset Password.

After logging in with the new password, administrators can change their password by clicking **Change Password** in the Admin Portal. In order to do so, they will have to correctly answer to the security question they entered on their first login.



3.2.4 Deleting Administrator Accounts

When an administrator account is no longer needed it should be deleted from the system. Deletion is permanent. If you are not sure about deleting an administrator, consider resetting the administrator's password.

To delete an administrator:

- 1. Log in to the Admin Portal.
- 2. Click Administrators.
- 3. Find the administrator in the **Administrators** table, and then click **Delete** for that administrator.
- 4. Click **OK** in the confirmation window.



4.0 Configuring Your Campus

To configure a campus, you need to specify the buildings, wings, floors, and rooms that make up your site.

The following topics are covered in this chapter:

- Campus
- Entering Your Campus Information
- Managing Buildings
- Managing Wings
- Managing Floors
- Managing Rooms



4.1 Campus

Your campus is the site where the MiCare Central server and MiCare devices are installed. There can only be one campus for each installation of Central. Within the campus, however, you can have one or more buildings, each of which can have one or more wings, floors, and rooms.

While configuring your campus, you must upload images for the campus map, the buildings, and the floors. Uploading these images makes it possible for the Nurse Call System to locate residents and attendants in Dashboard.

4.2 Entering Your Campus Information

The campus screen contains the contact details for your campus. It is here that address, telephone, and personnel information for the campus are found. When you are configuring your campus, you must upload an image file of the campus map. The campus map allows you to specify where buildings are located on your campus.

To enter your campus information:

- 1. From the Admin Portal, click Campus.
- 2. Type in the information for your campus. Fields with a red asterisk are required.
- 3. Scroll down to the **Campus Image** section.
- 4. Click Select.
- In the File Upload window, browse to the location of the image file for the campus, select it, and then click Open.
- 6. Click Save Campus.

You can update the information for your campus at any time by returning to the Campus screen in the Admin Portal, making your changes, and then clicking **Save Campus**.

4.3 Managing Buildings

A campus is made up of one or more buildings. After you add a building, you can add wings, floors, and rooms to it. You can optionally locate your building on the campus map by placing a location icon for the building on the campus map.

4.3.1 Adding a Building

Each building has its own contact details, such as address, phone number, and building manager. When you add a building to the campus you must upload an image of the building to Central.

To add a building to your campus:

- 1. From the Admin Portal, click **Buildings**.
- 2. Click Add New Building.
- Type in the information for your building. Fields with a red asterisk are required.



- 4. Scroll down to the **Locate Building** section.
- 5. In the Building Image section, click Select.
- 6. In the **File Upload** window, browse to the location of the image file for the building, select it, and then click **Open**.
- 7. Click Save Building.

After saving your building you are taken to the Buildings screen and the new building is listed in the Buildings table.

4.3.2 Locating a Building on the Campus Map

You can place a marker showing where a building is located on the campus map. When you locate your building, a location icon (\star) is placed on the campus map. Locating buildings on the campus map makes it easier to see where alerts are happening.

To locate your building on the campus map:

- 1. From the Admin Portal, click Buildings.
- 2. Find the building you want to locate in the **Buildings** table, and then click **Edit** for that building.
- 3. Scroll down to the Locate Building section.
- 4. In the **Campus Image** area, find the location of your building on the campus image, and then click on that location.
 - A location icon (\bigstar) is placed on the map where you clicked. If you want to change the location of the building, click on another location.
- 5. Click Save Building.

4.3.3 Editing a Building

To edit a building:

- 1. From the Admin Portal, click **Buildings**.
- 2. Find the building in the Buildings table, and then click Edit for that building.
- 3. Make your changes to the building information.
- 4. Click Save Building.

4.3.4 Deleting a Building

Before deleting a building, you must first delete all the building's rooms, floors, and wings.

To delete a building from your campus:

- 1. From the Admin Portal, click Buildings.
- 2. Find the building in the **Buildings** table, and then click **Delete** for that building.
- 3. Click **OK** in the confirmation window.



4.4 Managing Wings

Wings are used to separate buildings into one or more sections. After you add a wing to a building, you can add floors to the wing, and then rooms to the floors. To access the wing of a building, edit the building that contains the wing.

4.4.1 Adding a Wing

Each wing has contact information for the person in charge of the wing. After you have added a wing to a building, you can start adding floors to the wing.

To add a wing to a building:

- 1. From the Admin Portal, click Buildings.
- 2. In the **Buildings** table, find the building you want to add the wing to, and then click **Edit** for that building.
- 3. Scroll down to the **Wings** section, and then click **Add Wings**.
- Type in the information for the wing.
 Fields with a red asterisk are required.
- 5. Click Save Wing.

4.4.2 Locating a Wing on the Building Image

You can place a marker on the building image to show where a wing is on its building.

To locate a wing on the building image:

- 1. From the Admin Portal, click Buildings.
- 2. In the **Buildings** table, find the building that contains the wing you want to locate, and then click **Edit** for that building.
- 3. Scroll down to the **Locate Wing** section, find the wing on the building image, and then click on that location.
 - A location icon (\bigstar) is placed on the building image where you clicked. If you want to change the location of the marker, click on another location.
- 4. Click Save Wing.

4.4.3 Editing a Wing

To edit a wing:

- 1. From the Admin Portal, click **Buildings**.
- 2. In the **Buildings** table, find the building that contains the wing you want to edit, and then click **Edit** for that building.
- 3. Scroll down to the **Wings** table.
- 4. Find the wing that you want to edit, and then click **Edit** for that wing.
- 5. Make your changes to the wing information.
- 6. Click Save Wing.



4.4.4 Deleting a Wing

You can delete a wing when it is no longer needed. Before you can delete a wing from a building, you must first delete all of the rooms and floors that the wing contains.

To delete a wing:

- 1. From the Admin Portal, click Buildings.
- 2. In the **Buildings** table, find the building that contains the wing you want to delete, and then click **Edit** for that building.
- 3. Scroll down to the Wings table.
- 4. Find the wing that you want to delete, and then click **Delete** for that wing.
- Click **OK** in the confirmation window.

4.5 Managing Floors

Floors are located in wings. After you add a floor to a wing, you can add rooms to the floor.

4.5.1 Adding a Floor

When you add a floor to a wing, you must provide a name and a floor plan for that floor. If a nursing station is present on the floor, you must also provide contact information for the nursing station. Floors are added to wings by editing the wing that contains the floor.

To add a floor to a wing of a building:

- 1. From the Admin Portal, click Buildings.
- 2. In the **Buildings** table, find the building you want to add the floor to, and then click **Edit** for that building.
- 3. Scroll down to the **Wings** section, find the wing you want to add the floor to, and then click **Edit** for that wing.
- 4. Scroll down to the Floors section, and then click Add Floor.
- 5. Type in the information for the floor. Fields with a red asterisk are required.
- 6. If there is a nursing station on the floor, select the **Station Present** check box in the **Nursing Station** section, and then type in the information for the nursing station.
- 7. Scroll down to the Floor Image section, and then click Select.
- 8. In the **File Upload** window, browse to the location of the image file for the floor, select it, and then click **Open**.
 - The image must be a JPEG and at least 640 pixels wide by 329 pixels high.
- 9. Click Save Floor.



4.5.2 Editing a Floor

To edit the information for a floor:

- 1. From the Admin Portal, click Buildings.
- 2. In the **Buildings** table, find the building with the floor you want to edit, and then click **Edit** for that building.
- 3. Scroll down to the **Wings** section, find the wing with the floor you want to edit, and then click **Edit** for that wing.
- Scroll down to the Floors section, find the floor you want to edit, and then click Edit for that floor.
- 5. Make your changes to the floor information.
- Click Save Floor.

4.5.3 Deleting a Floor

You can delete a floor when it is no longer needed. Before you can delete a floor from a wing, you must first delete all of the rooms that the floor contains.

To delete a floor:

- 1. From the Admin Portal, click Buildings.
- 2. In the **Buildings** table, find the building with the floor you want to delete, and then click **Edit** for that building.
- Scroll down to the Wings section, find the wing with the floor you want to delete, and then click Edit for that wing.
- Scroll down to the Floors section, find the floor you want to delete, and then click Delete for that floor.
- 5. Click **OK** in the confirmation window.

4.6 Managing Rooms

You can add one or more rooms to a floor. After adding a room you can assign MiCare devices to the room (see Managing Devices on page 43). Assigning a device to a room allows Central to identify the room where an alert is raised by a device. It also helps Central to locate residents and attendants using mobile MiCare devices.

When you add a room, you must select the type of room it is. The types of rooms you can add are the following.

- Common Room: A common area such as a dining room or a lobby.
- Room: A private room such as a resident room.

You can optionally locate the room on the floor plan. Locating rooms on the floor plan makes it easier to see where alerts are happening on the Dashboard home screen.



4.6.1 Adding a Room

Rooms are added to floors by editing the floor that the room is located on. Every room must have a unique name. If the room is a private room, you must also enter the number of beds in the room.

To add a room to a floor:

- 1. From the Admin Portal, click Buildings.
- 2. In the **Buildings** table, find the building you want to add the room to, and then click **Edit** for that building.
- 3. Scroll down to the **Wings** section, find the wing you want to add the room to, and then click **Edit** for that wing.
- 4. Scroll down to the **Floors** section, find the floor you want to add the room to, and then click **Edit** for that floor.
- 5. Scroll down to the **Rooms** section, and then click **Add Room**.
- Type in the information for the room.Fields with a red asterisk are required.
- 7. If you selected **Room** for the Room Type, select the number of beds in the room. The number of beds must be 1 or more.
- 8. Click Save Room.

4.6.2 Locating a Room on the Floor Plan

You can place a marker on a floor plan to show where a room is located.

To locate a room on its floor plan:

- 1. From the Admin Portal, click Buildings.
- 2. In the **Buildings** table, find the building that contains the room you want to locate, and then click **Edit** for that building.
- Scroll down to the Wings table, find the wing that contains the room you want to locate, and then click Edit for that wing.
- 4. Scroll down to the **Floors** table, find the floor that contains the room you want to locate, and then click **Edit** for that floor.
- 5. Scroll down to the **Rooms** table, find the room that you want to locate, and then click **Edit** for that room.
- 6. Scroll down to the **Locate Room** section, find the room on the floor plan, and then click on that location.
 - A location icon (\star) is placed on the floor plan where you clicked. If you want to change the location of the room, click on the new location.
 - If there is a MiCare device in the room, place the icon as close to where the device is placed in the room as possible. See Assigning a Device on page 46.
- 7. Click Save Room.



4.6.3 Editing a Room

To edit the information for a room:

- 1. From the Admin Portal, click Buildings.
- 2. In the **Buildings** table, find the building with the room you want to edit, and then click **Edit** for that building.
- 3. Scroll down to the **Wings** section, find the wing with the room you want to edit, and then click **Edit** for that wing.
- 4. Scroll down to the **Floors** section, find the floor with the room you want to edit, and then click **Edit** for that floor.
- Scroll down to the **Rooms** section, find the room you want to edit, and then click **Edit** for that room.
- 6. Make your changes to the room information.
- 7. Click Save Room.

4.6.4 Deleting a Room

To delete a room from a building:

- 1. From the Admin Portal, click Buildings.
- 2. In the **Buildings** table, find the building with the room you want to delete, and then click **Edit** for that building.
- Scroll down to the Wings section, find the wing with the room you want to delete, and then click Edit for that wing.
- Scroll down to the Floors section, find the floor with the room you want to delete, and then click Edit for that floor.
- Scroll down to the **Rooms** section, find the room you want to delete, and then click **Delete** for that floor.
- 6. Click **OK** in the confirmation window.



5.0 Managing Attendants

Attendants are caregivers in the Nurse Call System. At the beginning of each shift, the attendants start their shifts in the Shift Manager. From Dashboard the attendant can view and respond to alerts generated by MiCare devices. In addition, the Central server can call, email, or page attendants when an alert is raised on your site.

The following topics are covered in this chapter:

- Attendants
- Adding an Attendant
- Editing an Attendant
- Changing the PIN for an Attendant
- Deleting an Attendant



5.1 Attendants

The **Attendants** screen allows you to manage the attendants at your site. From this screen you can see the attendant's status, add attendants, edit attendants' information, change an attendant's four-digit personal identification number (PIN), and delete an attendant.

5.2 Adding an Attendant

In order to log in to Dashboard, an attendant needs be added to the MiCare Central Station and the attendant must have a unique PIN. A unique PIN is automatically generated by Central when you add an attendant.

To add an attendant:

- 1. From the Admin Portal, click Attendants.
- 2. Click Add New Attendant.
- 3. Type in the information for the attendant. Fields with a red asterisk are required.

If you provide one of or both of the Email and SMS Email fields, you can define a rule to send a message to the attendant when alerts are raised. For information on defining rules, see Defining Rules on page 51.

4. Click Save Attendant.

You must give your attendants their PIN numbers in order for them to log in to Dashboard. If you forget an attendant's PIN, you can find the PIN for that attendant by going to the **Attendants** screen, finding the attendant in the **Attendants** table, and then clicking **Edit** for the attendant.

5.3 Editing an Attendant

To edit the information for an attendant:

- 1. From the Admin Portal, click **Attendants**.
- 2. Find the attendant you want to edit, and then click Edit for that attendant.
- 3. Make your changes to the attendant information.
- 4. Click Save Attendant.

5.4 Changing the PIN for an Attendant

Attendants use their PIN to log in to Dashboard. Administrators can change the PIN for an attendant whenever it is necessary. Note that you cannot enter a PIN manually. The Central system generates an unassigned PIN for you.

To change the PIN for an attendant:

- 1. From the Admin Portal, click **Attendants**.
- 2. Find the attendant you want to change the PIN for in the **Attendants** table, and then click **Edit** for that attendant.



- 3. Click Generate PIN.
- 4. Click OK.
- 5. Click Save Attendant.

5.5 Deleting an Attendant

You can delete an attendant from Central when it is necessary. If you are not sure about deleting an attendant, consider changing the PIN for the attendant (see section 5.4 above).

To delete an attendant:

- 1. From the Admin Portal, click Attendants.
- 2. Find the attendant you want to delete, and then click **Delete** for that attendant.
- 3. Click **OK** in the confirmation window.



6.0 Managing Residents

Residents can either be hospital patients or residents. You can enter all of the information associated with a resident into the MiCare Nurse Call System, including contact information, medications reminders, and check-in requirements.

The following topics are covered in this chapter:

- Residents
- Adding a Resident
- Adding Medication Reminders for a Resident
- Adding Family Contacts for a Resident
- Adding Medical Contacts for a Resident
- Editing Resident Information
- Deleting a Resident



6.1 Residents

Resident information is managed using the **Residents** screen in the Admin Portal. You can enter the following information for a resident:

- General: Contact details (for example, name, address, and email) and an image file for the resident.
- Check Ins: Days and times the resident is required to check in to Central. Residents that need to check in must have a device assigned to them and that device must have a rule that handles a failed patient check-in event.
- Health and medications: Notes relating to the resident's health, allergies, and medication.
- Medication reminders: A list of medications the resident is required to take. Medication reminders listed here are displayed in the daily Medication Reminders report (see Generating Resident Medication Reports on page 67).
- Family contacts: People that should be contacted in case of emergency.
- Family Doctors: Contact information for the resident's family doctors.
- Specialists: Contact information for the resident's specialists.

6.2 Adding a Resident

To add a new resident:

- From the Admin Portal, click Residents.
- 2. Click Add New Resident.
- Type in the general information for the resident. Fields with a red asterisk are required.
- 4. (Optional) If you have an image file for the resident, perform the following steps to upload the image.
 - a. Click Select.
 - b. In the **File Upload** window, browse to the location of the image file, select the image file, and then click **Open**.
- (Optional) If the resident is required to check in on a regular basis, scroll down to the Check In section, and then select the days of the week and the times the resident is required to check in to Central.

In order for the resident to be able to check in, you must also do the following:

- Assign a MiCare device for the resident to use for their check ins. For information on assigning a device to a resident, see Managing Devices on page 43.
- After assigning a device to the resident, define a failed patient check-in rule for that device. This creates an alert on Central when the resident misses a check in.
 For information on defining rules for a device, see Defining Rules on page 51.
- (Optional) If the resident has provided health, allergy, and medication information, scroll down to the **Health and Medications** section, and then enter the information.
- 7. Click Save Resident.



6.3 Adding Medication Reminders for a Resident

After adding a resident, you can add medication reminders for the resident. Medication reminder reports can be run and then given to nursing and care providers (see Generating Resident Medication Reports on page 67).

To add a medication reminder for a resident:

- 1. From the Admin Portal, click Residents.
- Find the resident that you want to generate the medication reminder for, and then click Edit.
- Scroll down to the Medication Reminders section.
- 4. Select Activate Medication Reminders for this Resident.
- 5. Click Add Medication Reminder.
- 6. Type in the information for the medication reminder, including at least one active day and at least one time for the medication reminder.

Fields marked with a red asterisk are required. When adding a reminder, note the following:

- To select a time, click the time view icon (), and then select the time.
- To add more reminder times, click the add icon () next to a reminder time.
- To delete a reminder time, click the delete icon () for the reminder time.

7. Click Save Reminder.

For information on how to run a medication reminders report, see section 11.5, Generating Resident Medication Reports, on page 67.

6.4 Adding Family Contacts for a Resident

After adding a resident you can add family contact information for that resident.

To add a family contact for a resident:

- 1. From the Admin Portal, click Residents.
- 2. Find the resident that you want to add a family contact for, and then click **Edit** for that resident.
- 3. Scroll down to the Family Contacts table, and then click Add Family Contact.
- Type in the information for the family contact.
 Fields marked with a red asterisk are required.
- 5. Click Save Contact.

6.5 Adding Medical Contacts for a Resident

After adding a resident you can add medical contacts for the resident. Medical contacts include family doctors and specialists.



To add a medical contact for a resident:

- 1. From the Admin Portal, click Residents.
- 2. Find the resident that you want to add a medical contact for, and then click **Edit** for that resident.
- 3. Depending on the type of contact, do one of the following:
 - If you are adding a family doctor, scroll down to the **Family Doctors** table, and then click **Add Family Doctor**.
 - If you are adding a specialist, scroll down to the Specialists table, and then click Add Specialist.
- 4. Type in the contact information for the family doctor or specialist. Fields marked with a red asterisk are required.
- Click Save Contact.

6.6 Editing Resident Information

To edit the information for a resident:

- 1. From the Admin Portal, click **Residents**.
- 2. Find the resident you want to edit in the **Residents** table, and then click **Edit** for that resident.
- 3. Make your changes to the resident information.
- 4. Click Save Resident.

6.7 Deleting a Resident

To delete a resident:

- 1. From the Admin Portal, click Resident.
- Find the resident that you want to delete in the Residents table, and then click Delete for that resident.
- 3. Click **OK** in the confirmation window.



7.0 Editing Global Device Templates

Each MiCare device in the Nurse Call System has a template by default. The **Global** screen lets you edit the templates. It is here that you can specify the common settings for each device type.



Attention: You must edit the global templates before you add devices.

This chapter covers the following topics:

- Coordinators, Routers, and End Devices
- Global Device Templates
- NC-2000 Patient Unit Global Template Settings
- NC-210 Beacon Global Template Settings
- NC-103 Pull Station Global Template Settings
- NC-220 ZF3 Global Template Settings
- NC-500 Pendant Global Template Settings



7.1 Coordinators, Routers, and End Devices

There are three types of wireless devices that make up the Nurse Call System, and which are used in templates.

- Coordinators (for example NC-2100K Coordinator Bundles): Coordinators connect
 to the Nurse Call System Central server through a USB connection. Their purpose is to
 transport messages back and forth between the Central server and the routers on the
 ZigBee wireless network.
- Routers (for example NC-210 Beacons and NC-2000 Patient Units): Routers
 communicate with the Nurse Call System Central server through the coordinators on the
 Nurse Call System. Routers also listen for messages from end devices on the system,
 which they then pass on to the Central server. Finally, routers come with ultrasound
 transmitters that are used to locate ultrasound-enabled end devices (pendants).
- End Devices (for example, the NC-103 Pull Stations and the NC-220-ZF3): End
 devices send messages about their status wirelessly to the ZigBee network. They do not
 communicate directly with the Central server. Their messages are instead passed on to
 the Central server through a router on the network.

7.2 Global Device Templates

You can edit device templates for each of the devices in the Nurse Call System.

For example, if all of your Patient Units have the same emergency phone numbers, you can enter these numbers once in the global device template for the Patient Unit. Every time a new Patient Unit is added to the Nurse Call System, the new Patient Unit will automatically be configured with the emergency numbers.

Device templates are set up in the Global screen on the Central Server. To access the Global screen, go to the Admin Portal, and then click Global. The MiCare devices that you can create global device templates for are the following:

- Patient Unit
- Beacon
- Pull Station
- ZF3
- Pendant
- Asset Tag (reserved for future use)
- Staff Badge (reserved for future use)

Details on how to configure each of these devices can be found in sections 7.3 to 7.7.

7.3 NC-2000 Patient Unit Global Template Settings

To access the configuration template for the Patient Unit, from the **Admin Portal**, click **Global**, and then click the **Configure** link for the Patient Unit entry in the Global Devices table.

The configuration template is broken up into the following categories:

• **General Configuration Options**: These are general settings for the Patient Unit, such as ultrasound transmitter settings, telephone settings, and dome light settings.



- **ZigBee**: These are settings related to the wireless ZigBee network, such as which channels to use and how often to attempt communication with the Coordinators in the system.
- Alerts: The rest of the sections on this page are related to the alerts that the Patient Unit
 raises when a call-point is activated. Call-points are activated by buttons (for example,
 Emergency, Code Blue, and Cancel), inputs, bed cords, and power loss.

Details on the settings for each of these categories are given in sections 7.3.2 to 7.3.4. Sections 7.3.5 and 7.3.6 describe how to edit a template for the Patient Unit and how to push that configuration to the Patient Units in your installation.

7.3.1 Restarting the Patient Unit

If you are experiencing problems with the Patient Unit, restart it.

To restart the Patient Unit

• Press the Cancel and Nurse Out buttons at the same time.

To reset the Patient Unit to factory default settings



Attention: Resetting should be performed only by a trained technician.

Press the Cancel and Staff Assist buttons at the same time.
 For information on the default settings, see 7.3.2 General Configuration Options below.

7.3.2 General Configuration Options

This section describes the options available in the general configuration setting for the Patient Unit.

Ultrasonic Power

This sets the volume on the ultrasound transmitter. In most cases, set to the highest power. Set to a lower power when two ultrasonic transmitters (Patient Unit or Beacon) are in the same room.

Settings range from 1 (lowest) to 4 (highest). The default is 4.

Ultrasonic Enable

All routers in the Nurse Call System have ultrasound transmitters. These transmitters are the primary method for locating mobile MiCare devices (the NC-500 Pendant) in your facility.

Select this option to enable the ultrasound transmitter. Clear this option to disable the ultrasound transmitter. Ultrasonic Enable is on by default.

Heartbeat

Every device on the Nurse Call System sends messages to Central to indicate that it is alive (that is, a heartbeat message). Set Heartbeat to the number of minutes between successive heartbeat messages. The default is 5 minutes.



Phone Line Enable

The Patient Unit can open a two-way voice communication channel between the room and another telephone. Voice communication is activated under any of the following conditions:

- A rule is triggered that requires a call to be made (see Chapter 10.0 Defining Rules on page 51).
- An attendant opens a voice communication channel for an alert through Dashboard.
- The Patient Unit has not received an alert acknowledgement from the Central Server. (That is, communication has been lost with Central.)
- The Persistent option is selected for the alert and the Phone Escalation Time timer has expired.

Select the Phone Line Enable option to allow the Patient Unit to initiate phone calls. If you enable this option, make sure that the unit is connected to a phone line. To not allow the Patient Unit to make calls, clear the Phone Line Enable option.

Phone Line Enable is off by default.

Supervised Inputs Enable

Each Patient Unit has four inputs for devices such as door contacts, flood detectors, and smoke detectors. These inputs can be installed with supervision. In order to supervise an input, the Patient Unit must know which inputs are supervised.

To let the Patient Unit know that an input is supervised, select the input's number.

Inputs are not supervised by default.

For more information on Patient Unit inputs and how to install them, see LT-2074, the MiCare Nurse Call System Installation Manual.

Dome Light Blink Period

Dome lights can be configured to either blink or stay on solid during an alert. The Dome Light Blink Period option sets the length of time, in milliseconds, that the dome lights turn on and off if the blink option is enabled (see the Dome Lights section in 7.3.4 Alerts on page 36). You can enter any value from 500ms to 4000ms. The default is 500ms.

Dial Attempts

This is the number of times that the Patient Unit tries to dial a phone number. Between dial attempts, the Patient Unit waits the amount of time set in the Redial Delay option.

If a call is not made after the Dial Attempts have been exhausted, the Patient Unit either dials the secondary emergency number (if there is one) or it escalates the alert to the next level. The levels are defined in the rule for the device (see 10.0 Defining Rules on page 51).

The default is 1.

Remote Cancel Enable

Select this option to allow nursing or care staff to cancel alerts remotely either through the MiCare Dashboard web interface or over the telephone. (To cancel an alert over the telephone, the attendant dials *9 on the telephone keypad after answering a call from a Patient Unit.)



Clear this option to not allow nursing and care staff to cancel alerts remotely. Remote Cancel Enable is on by default.

Phone Escalation Time

The Phone Escalation Time timer starts when an alert is triggered. If the alert is not cancelled before the end of the Phone Escalation Time, the Patient Unit dials the primary phone number (Phone #1) for the alert. In addition, if the Persistent option is set for the alert, the Patient Unit triggers the alert again. The default is 120 seconds.

Maximum Call Time

This is the maximum amount of time that the speech path stays open once a call has been started.

You can select a value from 0 to 30 minutes. The default is 0.

Redial Delay

This is the amount of time (in seconds) the Patient Unit waits before redialling a phone number. You can select a value from 5 to 15. The default is 0.

7.3.3 ZigBee

MiCare devices communicate wirelessly using the ZigBee protocol. This section describes the ZigBee communication options that you can set for the Patient Unit.

Always Dial

Select this option to enable ZigBee wireless communication (default). Clear this option to disable communication on the ZigBee network. This option is on by default.

If this option is disabled, then the **Phone Line Enable** option should be checked and a phone line should be connected.



Note: This option should **always** be enabled for all Patient Units. If ZigBee is disabled, then the only way of informing attendants of an alarm is through the phone lines.

ZigBee Retry Attempts

This option is related to the communication link between the Patient Unit and the Coordinators in the Nurse Call System. The Patient Unit sends all messages to the Coordinator, and then waits for an acknowledgement from Central. If an acknowledgement is not received within a certain time (Retry Delay), the Patient Unit resends the message to the Coordinator. ZigBee Retry Attempts is the number of times the Patient Unit tries to resend the message to the Coordinator.

After ZigBee Retry Attempts with the Coordinator, if the Patient Unit still hasn't received an acknowledgement, the Patient Unit assumes that it cannot communicate with Central. At this point the Patient Unit dials the emergency numbers (Phone #1 and Phone #2) for the alert.

The default is 1.

Retry Delay

This is the amount of time (in seconds) the Patient Unit waits before resending a message to the Coordinator. You can select a value from 1 to 10. The default is 1 second.



ZigBee Escalation Time

The ZigBee Escalation Time timer starts when an alert has been acknowledged. If the alert is not cancelled before the end of the ZigBee Escalation Time, the Patient Unit sends a message to Central to increase the escalation level for the alert. The default is 120 seconds.

LQI Threshold

The default method for locating mobile MiCare devices is through the ultrasound transmitter. However, if ultrasonic location fails, a secondary locating method based on the ZigBee Link Quality Indication (LQI) is used. The LQI measures the strength of the wireless signal between the mobile device and the router. The higher the LQI number, the closer the device is to the router, and therefore the more significant in determining the location of the device.

The Patient Unit uses the LQI Threshold setting to determine whether or not to send location information to the Coordinator. If the LQI from a device is less than the LQI Threshold, the Patient Unit does not send the device's LQI to the Coordinator. For typical installations, the default LQI Threshold of 16 is adequate.

You can set the LQI Threshold to any value from 0 to 255. The default is 16.

Channel Mask

Specify what ZigBee wireless channels the Nurse Call System uses. Under normal circumstances, you do not need to make any changes to the channels. By default, the channels are 15, 20, 25, and 26.

7.3.4 Alerts

The remaining sections in the Patient Unit template deal with the different types of alerts that the Patient Unit sends:

- Emergency Button residents press this button to call the attendant
- Nurse In/Out attendants use these buttons to track the time they spend in the room
- Cancel Button cancels an event
- Staff Assist Button attendants press this button to call for help
- Code Blue for life-threatening emergencies
- Button Stuck
- Phone Line Unplugged
- Input #1
- Input #2
- Input #3
- Input #4
- 1/4" Jack 1
- 1/4" Jack 2
- Maintenance used if the device needs maintenance or the room needs to be cleaned
- · Custom defined by the administrator
- External Power Lost

This section describes the options that are available for these alerts. Note that some alerts do not have all of these options. For example, the Nurse In/Out alert only has options for the Dome Lights.



Phone #1

This is the primary emergency number. The Patient Unit tries to dial this number first when it cannot communicate with Central.

Phone #2

This is the secondary emergency number. The Patient Unit dials this number when it cannot call the primary emergency number.

Persistent

Select this option to make the alert persistent. This option is off by default.

A persistent alert must be cancelled at the Patient Unit before the ZigBee Escalation Time expires. If the alert is not cancelled, the Patient Unit sends the alert again and escalates the alert level.

A not persistent alert only requires that the alert message be acknowledged by Central. Clear Persistent to make the alert not persistent.

Priority

If more than one alert is active at the same time, the alert with the highest priority takes precedence. For example, if two alerts are trying to open a two-way voice channel at the same time, the alert with the higher priority will take control of the phone line first.

You can select any value from 1 (lowest) to 9 (highest) for the priority. The Cancel alert should always have the highest priority. By default, the Cancel button and the Nurse button have priorities of 9. The other buttons have priorities of 5.

Mute

Select this option to mute the microphone on the Patient Unit when the alert is active. This option is off by default.

Silent Dial

Select this option to mute the dialing process when the Patient Unit makes a call to a phone line. This option is off by default.

Dome Lights

To have a dome light turn on during an alert, select the dome light in the **Enable** section.

If you want a dome light to blink when it is turned on, select the **Blink** option for that dome light.

These options are disabled by default.

7.3.5 Editing a Patient Unit Global Template

To edit a Patient Unit global template:

- 1. From the Admin Portal, click **Global**.
- 2. Click the **Configure** link for the Patient Unit entry in the Global Devices table.
- 3. Set the global options for the Patient Units in your installation. For information on these options, see sections 7.3.2 to 7.3.4.



4. Click Save Configuration.

7.3.6 Pushing the Patient Unit Global Template

If you need to make global changes to all of the Patient Units in your site, you can do it by pushing a new configuration from the Global screen.

To push a Patient Unit global template:

- 1. From the Admin Portal, click Global.
- 2. Click the Configure link for the Patient Unit entry in the Global Devices table.
- 3. Make the changes to the Patient Unit template.
- 4. Click Push Configuration to All Devices.
- 5. If any of the Patient Units require settings that are different from the global template, make the configuration changes for those Patient Units in the Devices screen. See Chapter 8.0, Managing Devices, on page 43 for information on configuring devices.

7.4 NC-210 Beacon Global Template Settings

To access the configuration template for the Beacon, from the **Admin Portal**, click **Global** and then click the **Configure** link for the Beacon entry in the Global Devices table.

7.4.1 Main Configuration

Ultrasonic Power

This sets the volume on the ultrasound transmitter. In most cases, set to the highest power. Set to a lower power when two ultrasonic transmitters (Patient Unit or Beacon) are in the same room.

Settings range from 1 (lowest) to 4 (highest). The default is 4.

Ultrasonic Enable

All routers in the Nurse Call System have ultrasound transmitters. These transmitters are the primary method for locating mobile MiCare devices (the NC-500 Pendant) in your facility.

Select this option to enable the ultrasound transmitter. Clear this option to disable the ultrasound transmitter. Ultrasonic Enable is on by default.

7.4.2 ZigBee

LQI Threshold

The default method for locating mobile MiCare devices is through the ultrasound transmitter. However, if ultrasonic location fails, a secondary locating method based on the ZigBee Link Quality Indication (LQI) is used. The LQI measures the strength of the wireless signal between the mobile device and the router. The higher the LQI number, the closer the device is to the router, and therefore the more significant in determining the location of the device.

The Beacon uses the LQI Threshold setting to determine whether or not to send location information to the Coordinator. If the LQI from a device is less than the LQI Threshold, the Beacon does not send the device's LQI to the Coordinator. For typical installations, the default LQI Threshold of 16 is adequate.



You can set the LQI Threshold to any value from 0 to 255. The default is 16.

Channel Mask

Select the ZigBee wireless channels the Nurse Call System uses. Under normal circumstances, you do not need to make any changes to the channels. By default, the channels are 15, 20, 25, and 26.

7.4.3 Creating a Beacon Global Template

To create a Beacon template:

- 1. From the Admin Portal, click Global.
- 2. Click the **Configure** link for the Beacon entry in the Global Devices table.
- 3. Set the global options for the Beacons in your installation. For information on these options, see sections 7.4.1 and 7.4.2.
- 4. Click Save Configuration.

7.4.4 Pushing the Beacon Global Template

If you need to make global changes to all of the Beacons in your site, you can do it by pushing a new configuration from the Global screen.

To push a Beacon global template:

- 1. From the Admin Portal, click Global.
- 2. Click the **Configure** link for the Beacon entry in the Global Devices table.
- 3. Make the changes to the Beacon template.
- 4. Click Push Configuration to All Devices.
- 5. If any of the Beacons have settings that are different from the global template, make the configuration changes for those Beacons in the Devices screen. See Chapter 8.0, Managing Devices, on page 43 for information on configuring devices.

7.5 NC-103 Pull Station Global Template Settings

To access the configuration template for the Pull Station, from the **Admin Portal**, click **Global** and then click the **Configure** link for the Pull Station entry in the Global Devices table.

7.5.1 Main Configuration

Heartbeat

Every device on the Nurse Call System sends messages to Central to indicate that it is alive (that is, a heartbeat message). Set Heartbeat to the number of minutes between successive heartbeat messages. The default is 5 minutes.

Delay between Attempts (sec)

This is the amount of time (in seconds) that the Pendant waits before retrying to send a message to the central server. The default is 7.



Remote Cancel Enable

Select this option to allow nursing or care staff to cancel alerts remotely through the MiCare Dashboard web interface. This option is enabled by default.

Clear this option to not allow nursing and care staff to cancel alerts remotely.

Number of Attempts

This is the number of times that the Pendant tries to send its message to the central server. The default is 3.

7.5.2 Creating a Pull Station Template

To create a Pull Station template:

- 1. From the Admin Portal, click Global.
- 2. Click the **Configure** link for the Pull Station entry in the Global Devices table.
- 3. Set the global options for the Pull Stations in your installation. For information on these options, see section 7.5.1.
- 4. Click Save Configuration.

7.5.3 Updating a Pull Station's Configuration

The Central server cannot push a configuration change to end devices like the Pull Station. Each Pull Station must make a request for a configuration update from Central.

To update the configuration for a Pull Station:

- 1. Press and hold the red Pull Station button until the red LED turns on solid (approximately 5 seconds).
- 2. Release the red Pull Station button.

If the LED on the Pull Station flashes red once and then continuously flashes amber, the Pull Station is in maintenance mode and is not configured. Repeat the previous steps until the Pull Station is properly configured.

7.6 NC-220 ZF3 Global Template Settings

To access the configuration template for the ZF3, from the **Admin Portal**, click **Global** and then click the **Configure** link for the ZF3 entry in the Global Devices table.

7.6.1 Main Configuration

Heartbeat

Every device on the Nurse Call System sends messages to Central to indicate that it is alive (that is, a heartbeat message). Set Heartbeat to the number of minutes between successive heartbeat messages. The default is 5 minutes.

Delay between Attempts (sec)

This is the amount of time (in seconds) that the Pendant waits before retrying to send a message to the central server. The default is 7.



Remote Cancel Enable

Select this option to allow nursing or care staff to cancel alerts remotely through the MiCare Dashboard web interface. This option is enabled by default.

Clear this option to not allow nursing and care staff to cancel alerts remotely.

Number of Attempts

This is the number of times that the Pendant tries to send its message to the central server. The default is 3.

7.6.2 Creating a ZF3 Global Template

To create a ZF3 template:

- 1. From the Admin Portal, click Global.
- 2. Click the **Configure** link for the ZF3 entry in the Global Devices table.
- 3. Set the global options for the ZF3s in your installation. For information on these options, see section 7.6.1.
- 4. Click Save Configuration.

7.6.3 Updating a ZF3's Configuration

The Central server cannot push a configuration change to end devices like the ZF3. Each ZF3 must make a request for a configuration update from Central.

To update the configuration for a ZF3:

- 1. Press and hold the cancel button on the ZF3 until the red LED turns on solid (approximately 5 seconds).
- 2. Release the cancel button.

If the LED on the ZF3 continuously flashes red, the ZF3 is in maintenance mode and is not configured. Repeat the previous steps until the ZF3 is properly configured.

7.7 NC-500 Pendant Global Template Settings

To access the configuration template for the Pendant, from the **Admin Portal**, click **Global** and then click the **Configure** link for the Pendant entry in the Global Devices table.

7.7.1 Main Configuration

Ultrasonic Enable

The ultrasound transmitter is used as the primary method for locating Pendants in your facility.

Select this option to enable the ultrasound transmitter. Clear this option to disable the ultrasound transmitter. Ultrasonic Enable is on by default.

Heartbeat

End devices must send their location at regular intervals to Central. The main locating method is ultrasonic location. The end device listens for an Ultrasonic ID from the nearest router, and



then sends that ID in a location message to Central. The Heartbeat determines how often (in minutes) the Pendant listens for an Ultrasonic ID and then updates its location to Central.

Select a value from 0 to 99,999. The default is 5 minutes.

Number of Attempts

This is the number of times that the Pendant tries to send its message to the central server. The default is 3.

Remote Cancel Enable

Select this option to allow nursing or care staff to cancel alerts remotely through the MiCare Dashboard web interface. This option is enabled by default.

Clear this option to not allow nursing and care staff to cancel alerts remotely.

Delay between Attempts (sec)

This is the amount of time (in seconds) that the Pendant waits before retrying to send a message to the central server. The default is 7.

7.7.2 Creating a Pendant Global Template

To create a Pendant template:

- 1. From the Admin Portal, click Global.
- 2. Click the **Configure** link for the Pendant entry in the Global Devices table.
- 3. Set the global options for the Pendants in your installation. For information on these options, see section 7.7.1.
- 4. Click Save Configuration.

7.7.3 Updating a Pendant's Configuration

The Central server cannot push a configuration change to end devices like the Pendant. Each Pendant must make a request for a configuration update from Central.

To update the configuration for a Pendant:

- 1. Press and hold the main Pendant button until the red LED turns on solid (approximately 5 seconds).
- Release the main Pendant button.

If the LED on the Pendant flashes red once and then continuously flashes amber, the Pendant is in maintenance mode and is not configured. Repeat the previous steps until the Pendant is properly configured.



8.0 Managing Devices

In order for a device to send alarms to Central, the device has to be added to Central and configured. Devices are added in the **Devices** screen of Central. After adding your devices, you can assign them to rooms, residents or attendants. You must also enter ultrasonic IDs for Patient Units and Beacons.

This chapter covers the following topics:

- Devices
- Adding a Device
- Assigning a Device
- Assigning an Ultrasonic ID to Patient Units and Beacons
- Retrieving the Patient Unit's Log File
- Editing a Device
- Deleting a Device



8.1 Devices

In order for a device to send alarms to the MiCare Central Station (Central), the device has to be added to Central and configured. Devices are added in the **Devices** screen of Central. After adding your devices, you can assign them to rooms, residents or attendants. The types of devices you can add are the following.

- NC-2000 Patient Unit
- NC-500 Pendant
- NC-103 Pull Station
- NC-210 Beacon
- NC-220 ZF3

This chapter covers how to add, assign, and delete devices.

This chapter does not cover how to configure individual devices. Details on how to configure devices can be found in Chapter 7.0 Editing Global Device Templates on page 31.

8.2 Adding a Device



Note: Power on all devices before adding them to Central.

All devices start communicating to Central when they turn on. To add a device to Central, you need to know its serial number and where the device is installed. You also need to run Discovery Mode on the MiCare processor. If you do not have this information, contact your MiCare Nurse Call System installer.

To add a new device:

- 1. Log in to the computer that runs the MiCare processor.
- 2. In the MiCare processor, click the **Settings** tab.
- 3. Select **60** seconds in the **Timeout** menu. This is the number of minutes that discovery mode will be active.
- 4. Click Start.



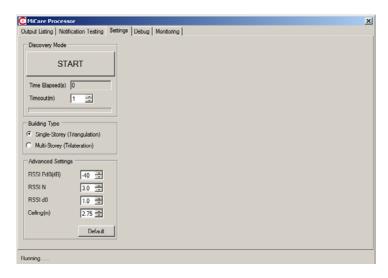


Figure 5 The Settings tab

- 5. Press any button on the device so that it communicates with the MiCare processor.
- 6. Click the Output Listing tab and confirm that the MAC address of the devices appears.

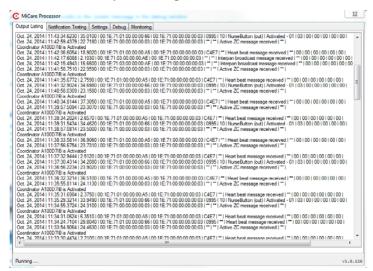


Figure 6 The Output Listing Tab

- 7. From the Admin Portal, click **Devices**.
- 8. Click New Detected Devices.

The **New Devices** screen opens. It may take a few minutes the new devices to be detected. New devices appear in the list.

Details on the configuration options for each device type can be found in the appropriate section in Chapter 7.0, Editing Global Device Templates, on page 31.

- For a Pendant, see section 7.7.3, Updating a Pendant's Configuration, on page 42.
- For a Pull Station, see section 7.5.3, Updating a Pull Station's Configuration, on page 40.
- For a ZF3, see section 7.6.3, Updating a ZF3's Configuration, on page 41.



8.3 Assigning a Device

You must assign all MiCare devices to one of the following entities in Central:

- Rooms
- Attendants
- Equipment (reserved for future use)
- Residents

To assign a device:

- 1. From the Admin Portal, click **Devices**.
- 2. Click **Assign** in the row of the device that you want to assign.
- Select the type of entity you want to assign the device to from the Assign To list. You can select from the following options:
 - Attendant
 - Equipment (reserved for future use)
 - Resident
 - Room
- 4. Select the attendant, resident, or room from the list in the **Select** section.
- Click Assign Device.

The **Assigned Device** screen opens. The newly assigned device is listed here.

8.4 Assigning an Ultrasonic ID to Patient Units and Beacons

Each Patient Unit and Beacon must have a unique ultrasonic ID. You must enter the ultrasonic ID in the **Devices** screen.

To assign an ultrasonic ID:

- 1. From the Admin Portal, click **Devices**.
- 2. Find the Patient Unit or Beacon you want to assign an ultrasonic ID to, and then click **Configure** for that device.
- 3. Enter a number between 1 and 4095 in the Ultrasonic ID field.
- 4. Click Save Configuration.

Repeat these steps for every Patient Unit and Beacon in the system. Enter a different number for each device.

8.5 Retrieving the Patient Unit's Log File

You can retrieve a log of the last 72 events recorded by a Patient Unit.



To retrieve a Patient Unit's log file:

- 1. From the Admin Portal, click **Devices**.
- 2. Find a Patient Unit, and then click **Configure** for that device.
- 3. Click Retrieve Log File.

The Admin Portal downloads a text file called **device.log** that contains the last 72 events recorded by the Patient Unit.

8.6 Editing a Device

You can edit a device's settings by making configuration changes in Central and saving them. If the device is an end device (for example, Pendant or a Pull Station), you must also manually update the device.

To configure a device:

- 1. From the Admin Portal, click **Devices**.
- 2. Find the device you want to edit in the **Devices** table, and then click **Configure** for that device.
- 3. Make the configuration changes for the device.
- 4. Click Save Configuration.

If the device you configured was a router, your configuration changes are automatically sent to the device. No further configuration is required.

If your device is an end device, then you must manually update the device's configuration. For instructions on how to update an end device, refer to the following sections.

- For a Pendant, see section 7.7.3, Updating a Pendant's Configuration, on page 42.
- For a Pull Station, see section 7.5.3, Updating a Pull Station's Configuration, on page 40.
- For a ZF3, see section 7.6.3, Updating a ZF3's Configuration, on page 41.

8.7 Deleting a Device

To delete a device:

- 1. Log in to the Admin Portal.
- 2. Click Devices.
- 3. Find the device you want to delete in the **Devices** table, and then click **Delete** for that device.
- 4. Click **OK** in the confirmation window.



9.0 Creating Groups

You can associate members with a group. Groups can be made up of Attendants, Devices, Equipment, and Residents. Groups are a convenient way to associate a number of similar items or members. For example, if you need to notify more than one attendant during an emergency event, rather than creating separate rules for each attendant you can create a group with the attendants as its members, and then have the rule call the group.

This chapter covers the following topics:

- Creating a Group
- Editing a Group
- Deleting a Group



9.1 Creating a Group

Groups associate members from the Devices, Attendants, Equipment, and Residents lists. Adding members to a group makes it easy to notify multiple members from a Rule. For example, you can create a group of attendants that should be notified when the Code Blue button is pressed on a Patient Unit.

To create a group:

- 1. From the Admin Portal, click Groups.
- 2. Click Add New Notification Group.
- 3. In the **Name** text box, type the name of the group.
- 4. In the **Description** text box, type a description for the group.
- 5. If this is an attendant group, select **This is an attendant group** and then type in the following information:
 - Group Phone Number: the hunt group phone number for the attendant group.
 - Group Pager Number: the hunt group pager number for the attendant group
- 6. Select the type of member you want to add from the Member Type list.

You can select from the following member types:

- Attendant
- Device
- Equipment (reserved for future use)
- Resident

After you select the member type, a member list appears with the same name as your selection. For example, if you select **Device**, a **Device** member list appears that contains the devices in Central.

- 7. Select the member you want to add from the member list, and then click **Add to Group**.
- Repeat steps 6 and 7 for all of the members you want to add to the group.
- 9. Click Save Group.

9.2 Editing a Group

To edit a group:

- 1. From the Admin Portal, click Groups.
- 2. Find the group you want to edit, and then click **Edit** for that group.
- 3. In the Edit Notification Group screen, make your changes.
- To add a member, select a Member Type, select the member from the appropriate list, and then click Add to Group.
- 5. If you want to delete a member, click **Delete** for that member, and then click **OK** in the confirmation window.
- Click Save Group.



9.3 Deleting a Group

To delete a group:

- 1. From the Admin Portal, click **Groups**.
- 2. Find the group you want to delete, and then click **Edit** for that group.
- Delete all of the members in the group.
 You cannot delete a group that has members in it. To delete a member of a group, click Delete for that member, and then click OK in the confirmation window.
- 4. Click Groups.
- 5. Find the group you want to delete, and then click **Delete** for that group.
- 6. Click **OK** in the confirmation window.



10.0 Defining Rules

Rules specify what actions the MiCare Nurse Call System takes when events happen. To define a rule, you must specify what event triggers the rule, what actions to take, and how long to wait until the next action or escalation.

This chapter covers the following topics:

- Rules
- Event
- Escalations
- Creating a Rule
- Editing a Rule
- Disabling and Enabling a Rule
- Deleting a Rule



10.1 Rules

Rules specify what action or actions the Central server performs when an event happens on a device. Examples of events include the pushing of a button or an input becoming active.

When an event happens on a MiCare device, the Central server finds the rule for that event on that device, and then immediately performs the action for the lowest escalation level (Level 1) for that rule. Examples of actions include sending an alert to Dashboard, calling the nearest attendant, or calling an attendant group.

After the action has been performed, Central starts an escalation timer and then waits for the event to get cleared. The amount of time Central waits is determined by the Wait Duration setting for the current escalation level. If the event is not cancelled before the Wait Duration time, Central performs the action specified in the next escalation level, and then waits for that level's Wait Duration time. This process continues until the event is cancelled.

To access the Rules screen, log in to the Admin Portal, and then click **Rules**. This screen shows a list of all the rules defined for your installation.

From here, click **Add a New Notification Rules**. This is where you can set the following options for each rule:

- Event: Specify the device(s), event type, and other options for the rule.
- Escalations: Define the action and Wait Duration for each escalation level for the rule.
 Up to 20 escalations can be set for a rule.

The settings in the Event section are covered in section 10.2. The settings in the Escalations section are covered in sections 10.3 to 10.6. How to create, edit, and delete rules and escalations are covered in sections 10.7, 10.8, 10.10, and 10.11.

10.2 Event

In order to define what triggers a rule, set the following options in the Event section.

Name

Type the name for the rule in the **Name** box. Each rule must have a unique name.

This is the default rule

Select this option to make this the default rule for all devices. The default rule is triggered if no rule has been defined for an event on a device. You cannot specify a device type or event type for the default rule.



Attention: The default rule should never be triggered once an installation is complete. That is, each event type for each device type should have a rule defined. This option can be used as a test to find what events do not have a rule.



Device Type

Select the device type from the list of devices. You can choose from the following device types:

- Patient Unit
- Beacon
- Pull Station
- ZF3
- Pendant
- Asset Tag (reserved for future use)
- Staff Badge (reserved for future use)

The selection you make determines what device(s) (see Select Device (Group)) and what event (see Event Type) triggers the rule.

Select Device (Group)

This option lists all of the devices that match your Device Type selection. You can select All Devices, a group, or choose one of the devices from the list.

If you select All Devices, the rule applies to all of the devices on the system that match your Device Type. For example, if you selected Patient Unit for the Device Type, then selecting All Devices will apply the rule to all of the Patient Units in your system.

If you select a group, the rule applies only to that group of devices. See Chapter 9.0 Creating Groups on page 48.

If you select an individual device from the list, the rule applies only to that individual device.

i

Notes: The rule for an individual device takes precedence over the All Devices rule for that Device Type.

If more than one rule is defined for the same event on the same device, only one rule is fired. In order to avoid confusion, you should not have more than one rule defined for an event type on the same device.

Event Type

Select an event from this list. What event you can add to a rule depends on the Device Type. For more information on the event types for each device, see sections 10.2.2 to 10.3.

Rule is Active daily: ... To: ...

If you want the rule to be active only during certain times of the day, specify a start time and an end time for the rule. If you enter 0:00 for both the start time and the end time, the rule is always active.

Send pager message while the event is cleared

Select this option to have the Central server send a page to the attendant who clears an event in the Dashboard, either by declining or accepting the event.



Recycle

Select this option to have the rule start over again after all the escalation levels for the rule have expired and the event has not been cancelled. If you do not select Recycle, the alert will stay active at its highest priority level until it is cancelled.

10.2.1 Coordinator Bundle Event Types

- Failure from Disconnect: There is a USB failure on both coordinators.
- Failure from Heartbeat: The processor is not receiving heartbeat messages from either of the two coordinators.
- Warning from Disconnect (Active): There is a USB failure on the active coordinator.
- Warning from Disconnect (Standby): There is a USB failure on the standby coordinator.
- Warning from Flip: One of the coordinators has restarted, so the other coordinator has taken over.
- Warning from Heartbeat: The processor is not receiving heartbeat messages from the active coordinator.

10.2.2 Patient Unit Event Types

You can select from over 20 event types on the Patient Unit. These event types fall into the following groups: Buttons, Inputs, Communication, and Power.

Buttons

For the following buttons, the rule fires when the selected button is pressed:

- Emergency Button
- Code Blue Button
- Custom Button
- Maintenance Button
- Staff Assist Button

In addition to these events, the following events are related to the buttons on the Patient Unit:

- **Button Stuck**: this event is triggered when any button on the Patient Unit is stuck or held down for too long.
- Failed Patient Check-in: If the Patient Unit is assigned to a resident and the resident is required to check-in periodically, the rule fires when the resident does not check-in.



Note: The Patient Unit is normally assigned to a room and not a resident. For this event to fire, the Patient Unit must be assigned to a resident. Although **Failed Patient Check-in** is a valid event type for the Patient Unit, other MiCare devices are better suited for the resident check-in feature (for example, the NC-500 Pendant and the NC-220 ZF3).

Inputs

The following events are related to the inputs on the Patient Unit.

• 1/4" Jack 1-2: The rule fires when the input connected to the 1/4" Jack input is activated. The rule also fires when the input is removed from the 1/4" jack.



• Hard wired input 1-4: Select one of the 4 hard wired inputs on the Patient Unit. The rule fires when the input becomes active.

In addition to these events, the following events are related to the hard wired inputs on the Patient Unit:

Input 1-4 Supervision Fail: The rule fires when the Patient Unit detects a break in the
input's supervision circuit. The input must have a supervision circuit installed and the
input must be designated as supervised in the Device configuration screen for the
Patient Unit.

Communication

The following events are related to a loss or resumption of communication between the Patient Unit and the Nurse Call System's Coordinators.

- **Heartbeat Failed**: The rule fires when Central has not received a heartbeat message from the Patient Unit within a specified time.
- Phone line unplugged: If the Patient Unit has the Phone Line Enable option set (see section 7.3 NC-2000 Patient Unit Global Template Settings on page 32), the rule fires when the phone line is unplugged on the Patient Unit.
- Router Recovery: This event is only of interest to technologists servicing the Patient
 Unit. The Patient Unit resets itself when an internal traffic buffer fills up. The rule fires
 when the Patient Unit recovers from the reset.

Power

The following events are related to power loss on the Patient Unit. Power refers to the external power coming from both the Patient Unit's power supply and the UPS that the power supply is using. Battery refers only to the auxiliary battery connected to terminal CN8 on the Patient Unit. For details, see LT-1074 MiCare Nurse Call System Installation Manual.



Note: When the Patient Unit is on auxiliary battery power, the dome lights are not powered.

- **External Power Lost**: The rule fires when there is no external power going to the Patient Unit and the Patient Unit is only getting power from the auxiliary battery.
- Low Battery (20% Level): The rule fires when the auxiliary battery is running below 20% of its full charge.

10.2.3 Beacon Event Types

The following communication event can be selected for the Beacon:

- **Beacon Recovery**: The Beacon resets itself when an internal traffic buffer fills up. The rule fires when the Beacon recovers from the reset.
- **Heartbeat Failed**: The rule fires when Central has not received a heartbeat message from the Beacon within a specified time.

10.2.4 Pull Station Event Types

The event types for the Pull Station fall into the following groups: Buttons, Inputs, Communication, and Power.



Buttons

For the following buttons, the rule fires when the selected button is pressed:

- Emergency Button
- Staff Assist Button

In addition to these events, the following event is related to button activity on the Pull Station:

• **Failed Patient Check-in**: If the Pull Station is assigned to a resident and the resident is required to check-in periodically, the rule fires when the resident does not check-in.

i

The Pull Station is normally assigned to a room and not a resident. For this event to fire, the Patient Unit must be assigned to a resident. Although **Failed Patient Check-in** is a valid event type for the Pull Station, other MiCare devices are better suited for the resident check-in feature (for example, the NC-500 Pendant and the NC-220 ZF3).

Inputs

Note:

The following events are related to the inputs on the Pull Station.

- Call Cord: The rule fires when the call cord on the Pull Station is pulled.
- Input Button: The rule fires when the input connected to terminal TS1 of the Pull Station becomes active. For details on the terminals, see LT-1074 MiCare Nurse Call System Installation Manual

Communication

The following event is related to a loss of communication between the Pull Station and the Nurse Call System's Coordinators.

 Heartbeat - Failed: The rule fires when Central has not received a heartbeat message from the Pull Station within a specified time.

Power

The following event is related to the battery status on the Pull Station.

Low Battery: The rule fires when the batteries are low.

10.2.5 ZF3 Event Types

The event types for the ZF3 fall into the following groups: Inputs, Communication, and Power.

Inputs

The following events are related to the inputs on the ZF3.

- Input 1-2: The rule fires when the selected input (1 or 2) on the ZF3 becomes active.
- Failed Patient Check-in: If the ZF3 is assigned to a resident and the resident is required to check-in periodically, the rule fires when the resident does not check-in.

Communication

The following event is related to a loss of communication between the ZF3 and the Nurse Call System's Coordinators.



• **Heartbeat - Failed**: The rule fires when Central has not received a heartbeat message from the ZF3 within a specified time.

Power

The following event is related to the battery status on the ZF3.

• Low Battery: The rule fires when the battery is low.

10.2.6 Pendant Event Types

The event types for the Pendant fall into the following groups: Buttons, Communication, and Power.

Buttons

The following events are related to the button on the Pendant.

- Emergency Button: The rule fires when the emergency button is pressed.
- **Failed Patient Check-in**: If the Pendant is assigned to a resident and the resident is required to check-in periodically, the rule fires when the resident does not check-in.

Communication

The following event is related to a loss of communication between the Pendant and the Nurse Call System's Coordinators.

• **Heartbeat - Failed**: The rule fires when Central has not received a heartbeat message from the Pendant within a specified time.

Power

The following event is related to the battery status on the Pendant.

• Low Battery: The rule fires when the battery is low.

10.3 Escalations

The Escalations section is where you define what actions Central takes for the rule. Up to 20 escalations can be assigned to a rule, and you can define one action for each escalation. In order to define an escalation, you must set the following options:

- **Output Scenario**: This area is where you set the escalation level and the type of action to perform.
- **Target**: This is where you select the recipient of the action. For example, if the action is to make a phone call, this is where you specify which person to call.
- **Response**: This is where you set how long Central waits before triggering the next escalation level. This is also where you save the escalation.

See sections 10.4, 10.5, and 10.6 for more information on the options for these settings.

10.4 Output Scenario

The Output Scenario section defines what action to perform when an escalation is reached. To define an action for an escalation, set the escalation's priority level (Level) and the action to perform (Output Type).



When a rule is fired, the action for the lowest escalation level is performed first, and then the Central server waits for a response. A response is typically a cancellation at the device that set off the rule. If there is no response before the end of the escalation's Wait Duration, the Central server executes the action for the next escalation level for the rule.

10.4.1 Level

This option sets the priority level for the escalation. You can select a value from 1 to 20, with 1 having the lowest priority level.

It is recommended that priority levels be entered in numerical order starting from 1. To select a priority level for an escalation, select a value from the list.

10.4.2 Output Type

This option sets what action to perform for the escalation. The available actions are:

- Call
- Dashboard
- Device Output
- Email
- Pager
- SMS Email
- XML

For details on what each of these actions do and how to configure them, see the following sections.

Call

Select Call to have a Patient Unit phone an individual or a group.

From the **Send To** list in the **Target** section, select one of the following the call recipients:

- Attendant: Call one of the attendants in the system. Select the attendant from the Attendant list.
- Attendant Group: Call one of the attendant groups in the system. Select the attendant group from the Attendant Group list.
- Administrator: Call one of the administrators in the system. Select the administrator from the Administrator list.
- **New**: Call a number that is not in the system. Type the number to call in the Number box.

Dashboard

Select Dashboard to send the alert to the Dashboard screen so that all attendants can see (and respond to) the alert.

i

Note: Dashboard should be the level 1 escalation for all events that require an attendant.



When you select Dashboard, you must also select a target in the **Target** section. This forces the alert to the top of the target's alerts window in Dashboard. From the **Send To** list in the **Target** section, select the target from the following options:

- Attendant: Target the alert to one of the attendants in the system. Select the attendant from the Attendant list.
- Attendant Group: Target the alert to an attendant group. The alert is sent to all of the members in the attendant group. Select the attendant group from the Attendant Group list.

i

Note: Targets must be logged on to Dashboard in order for the alert to be placed at the top of their alerts window. Otherwise, the alert appears in the order it arrives at the Central server.

Device Output

Select Device Output to turn on one of the outputs connected to a Patient Unit or a group of Patient Units.

Select which output(s) to activate from the following list:

- Output 1
- Output 2
- Output 3
- Output 4

From the **Send To** list in the **Target** section, select the target(s) from the following options:

- Device: Activate the selected output(s) for one Patient Unit. Select the Patient Unit from the Device list.
- **Device Group**: Activate the selected output(s) on the Patient Units in a device group. Select the device group from the Device Group list.

Email

Select Email to send an email to an individual or a group.



Note: In order to use Email and SMS Email, you must have access to an SMTP server.

From the **Send To** list in the **Target** section, select the recipient from the following options:

- Attendant: Send the email to an attendant in the system. Select the attendant from the Attendant list.
- Attendant Group: Send the email to an attendant group in the system. Select the attendant group from the Attendant Group list.
- Administrator: Send the email to an administrator in the system. Select the administrator from the Administrator list.
- **New**: Send the email to a recipient that is not in the system. Type the recipient's email address in the Email box.



Type the contents of the email into the **Message** box.

Pager

Select Pager to page an individual or group.

From the **Send To** list in the **Target** section, select recipient from the following options:

- Attendant: Page an attendant in the system. Select the attendant from the Attendant list
- Attendant Group: Page an attendant group in the system. Select the attendant group from the Attendant Group list.
- New: Page a recipient that is not in the system. Type the new pager number in the Number box.

Type the pager message into the **Message** box.

SMS Email

Select SMS Email to send a text message to an individual or a group.



Note: In order to use Email and SMS Email, you must have access to an SMTP server.

From the **Send To** list in the **Target** section, select the recipient from the following options:

- Attendant: Send the text message to an attendant in the system. Select the attendant from the Attendant list.
- Attendant Group: Send the text message to an attendant group in the system. Select the attendant group from the Attendant Group list.
- Administrator: Send the text message to an administrator in the system. Select the administrator from the Administrator list.
- New: Send the text message to a recipient that is not in the system. Type the new SMS address in the Email box.

Type the contents of the text message into the **Message** box.

XML

Select XML to send an XML message to a device that accepts XML messages. The receiving device must be configured in the Central server.

From the XML Device list, select your installation's XML device from the following options:

- IP4610
- IP4625
- Slink
- TTS

Type or copy the contents of the XML message into the **Message** box in the **Target** section.



10.5 Target

The Target area is where you specify the person, device, or group that receives the action selected in Output Type.

What targets are available depends on your Output Type choice. For details on the Target options available for each Output Type, see section 10.4.2.

10.6 Response

The Response section is where you define how long an escalation level is active. To do this, set a Wait Duration value.

Wait Duration

This option specifies how long in minutes an escalation level is active before Central moves to the next escalation level. The Wait Duration can be set to any value from 0 to 9999.

To have more than one escalation activate at the same time, set the Wait Duration for the first escalation to 0, and then set a non-zero value for the last escalation.

10.7 Creating a Rule

To create a rule:

- 1. From the Admin Portal, select Rules.
- 2. Click Add New Notification Rule.
- 3. If this is to be the default rule, select **This is the default rule**, type a name into the **Name** box, and then go to step 5.
- In the Event section, set the following:
 - Name
 - Device Type
 - Select Device (Group)
 - Event Type

For details on these options, see section 10.2 on page 52.

- 5. Set the time period for which the rule is active in the **Rule is Active daily:** ... **To:** ... section.
- 6. If the rule should be restarted after Central has activated all of the rule's escalation levels, select **Recycle**.
- 7. Set the escalation(s) for the rule by doing the following:
 - a. Select the escalation level from the Level list.
 - Set the Output Type and Target for the escalation.
 For details on these options, see section 10.4.2 on page 58.
 - c. In the **Response** section, set the **Wait Duration** time for the escalation.
 - d. Click Save Escalation.

This saves the escalation and adds it to the **Escalation Summary** table. You **must** click **Save Escalation** in order to save the escalation. Saving the rule does



not save the escalation.

- e. Repeat steps a to d for all of the escalations you want to add to the rule.
- 8. Click Save & Continue.

10.8 Editing a Rule

To edit a rule:

- 1. From the Admin Portal, select Rules.
- 2. Find the rule you want to edit, and then click **Edit** for that rule.
- 3. Make your changes to what triggers the rule in the **Event** section. For details on these options, see section 10.2 on page 52.
- 4. If you want to edit escalations for the rule, do the following:
 - a. Find the escalation you want to edit in the **Escalation Summary** table, and then click **Edit** for that escalation.
 - b. Make your changes to the escalation.
 - c. Click Save Escalation.
 - d. Repeat steps a to c for all of the escalations you want to edit.
- 5. Click Save & Continue.

10.9 Disabling and Enabling a Rule

To disable a rule:

- 1. From the Admin Portal, select Rules.
- 2. Find the rule you want to disable, and then click **Disable** for that rule.

The word **Disable** changes to **Enable**. The rule is now disabled.

To enable a rule:

- 1. From the Admin Portal, select Rules.
- 2. Find the rule you want to enable, and then click **Enable** for that rule.

The word **Enable** changes to **Disable**. The rule is now enabled.

10.10 Deleting an Escalation

To delete an escalation:

- 1. From the Admin Portal, select Rules.
- 2. Find the rule that contains the escalation you want to delete, and then click **Edit** for that rule.
- 3. Find the escalation you want to delete in the **Escalation Summary** table, and then click **Delete** for that escalation.
- 4. Click **OK** in the confirmation window.
- 5. Click Save & Continue.



10.11 Deleting a Rule

When you delete a rule, Central deletes the rule along with all of its escalations.

To delete a rule:

- 1. From the Admin Portal, select Rules.
- 2. Find the rule you want to delete, and then click **Delete** for that rule.
- 3. Click **OK** in the confirmation window.



11.0 Running Reports

You can run reports to monitor your facility's performance or to generate maintenance and medication schedules.

The following topics are covered in this chapter:

- Reports
- Monitoring Facility Call Point Performance
- Monitoring Nurse Service Time
- Generating Device Maintenance Reports
- Generating Resident Medication Reports
- Generating Detailed Archived Alerts Reports
- Generating Summarized Archived Alerts Reports
- The Report Window



11.1 Reports

Run MiCare reports to either monitor the performance of your facility or to generate lists of daily tasks. To access the reports screen, log in to the Admin Portal and then click **Reports**. The types of reports that you can run in Central are the following:

- Facility Reports: generate a report detailing the response times for an event (see Section 11.2).
- Staff Reports: generate a report on how much time an attendant was in a room (see Section 11.3).
- Device Reports: generate a report on which devices require maintenance (see Section 11.4).
- Resident Reports: generate a list of medications that need to be dispensed for the day (see Section 11.5).
- Generating Detailed Archived Alerts Reports (see Section 11.6)
- Generating Summarized Archived Alerts Reports (see Section 11.7)

Once you have generated your report you can perform searches, save it, or print it. Information on the report window and its commands is found in Section 11.8 on page 69.

11.2 Monitoring Facility Call Point Performance

The Call Point Performance Report measures how your facility responded to call points (that is, events) raised on MiCare devices.

You can filter the output of the report in two ways.

The first filter is used to specify what the alert is assigned to. You can select one of the following options from the **Assigned to** list:

- Attendant: Report the response time(s) for an attendant.
- Equipment: Reserved for future use.
- Group: Report the response time(s) for a member of a group.
- Resident: Report the response time(s) for events related to a resident.
- Room: Report the response time(s) for events related to a room.

The second filter specifies a specific call point (that is, event) from the **Call Points** list.

To generate a call point performance report:

- 1. From the Admin Portal, click Reports.
- 2. In the Facility Reports section, click Callpoint Performance.
- 3. Enter the start date and time and the end date and time for the report in the **Start** and **End** boxes.

You can either enter these values directly or click **Open the calendar** () to select a date and then click **Open the time view** () to select a time.

- 4. Select the filters for the report by doing the following:
 - a. Select the filter type from the **Assigned to** list.



- b. Make a selection from the **Attendant**, **Equipment**, **Attendant Group**, **Resident**, or **Room** list.
- c. Select an event from the Call Point list.

To not apply any filter(s), leave the appropriate list blank. For example, if **Assigned to** is blank, then the report lists the response for all of the attendants, equipment, attendant groups, and rooms in your facility.

5. Click Run Report.

The report displays at the bottom of the Facility Report screen. For information on the report window (including how to save or print the report) see Section 11.8 on page 69.

11.3 Monitoring Nurse Service Time

The Nurse Activity Report measures the amount of time an attendant was in a room attending to a resident.

You can filter the output of the report by selecting one of the following options from the **Assigned to** list:

- Room: Report the time(s) any attendant was attending to an alert in the room.
- Attendant: Report the time(s) an attendant was in any room attending to an alert.
- Attendant Group: Report the time(s) a member of an attendant group was in any room attending to an alert.

The time is tracked from when the attendant presses the Nurse In button to when the nurse presses the Nurse Out button on a Patient Unit.

To generate a nurse activity report:

- 1. From the Admin Portal, click Reports.
- 2. In the Staff Reports section, click Nurse Service Time.
- 3. Enter the start date and time and the end date and time for the report in the **Start** and **End** boxes.

You can either enter these values directly or click **Open the calendar** () to select a date and then click **Open the time view** () to select a time.

- 4. Select the filters for the report by doing the following:
 - a. Select the filter type from the **Assigned to** list (that is, select Attendant, Attendant Group, or Room).
 - b. Make a selection from the **Attendant**, **Attendant Group**, or **Room** list.

To not apply any filter(s), leave the appropriate list blank. For example, if **Assigned to** is blank, then the report lists the nurse activity for all of the attendants, attendant groups, and rooms in your facility.

Click Run Report.

The Nurse Report displays at the bottom of the Nurse Activity Report screen. For information on the report window (including how to save or print the report) see Section 11.8 on page 69.



11.4 Generating Device Maintenance Reports

Run a device maintenance report to get a list of all the devices requiring maintenance for the day.

To generate a device maintenance report:

- 1. From the Admin Portal, click **Reports**.
- 2. In the Device Reports section, click Pending Device Maintenance.
- 3. Click Run Report.

The report displays at the bottom of the Maintenance Alerts Report screen. For information on the report window (including how to save or print the report) see Section 11.8 on page 69.

11.5 Generating Resident Medication Reports

Run a resident medication report to get a list of all the medications to dispense for the day.

To generate a resident medication report:

- 1. From the Admin Portal, click **Reports**.
- 2. In the Resident Reports section, click Resident Medication.
- 3. Click Run Report.

The report displays at the bottom of the Resident Medication Report screen. For information on the report window (including how to save or print the report) see Section 11.8 on page 69.

11.6 Generating Detailed Archived Alerts Reports

The detailed archived alerts report displays a report for the events that you specify during the time that you specify. Each event is listed separately, with its device MAC address, attendant name, status, time added, and time actioned.

To generate a detailed archived alerts report:

- From the Admin Portal, click Reports.
- 2. In the Archived Alerts Report section, click Detailed Archived Alerts Report.
- 3. Enter the start date and time and the end date and time for the report in the **Start** and **End** boxes.
 - You can either enter these values directly or click **Open the calendar** () to select a date and then click **Open the time view** () to select a time.
- 4. Select the filters for the report by unselecting the events that you do not want in the report. To not apply any filter(s), leave all the events selected.
 - Click the checkbox at the top of the list of events to unselect or select all the events at once.
- Click Run Report.



The Detailed Archived Alerts Report displays at the bottom of the screen. For information on the report window (including how to save or print the report) see Section 11.8 on page 69.

Table 1 Detailed Archived Alerts Report

Column	Description
Event	The type of event that triggered the alert. This includes a button press, or a low battery or technical fault.
Assigned To	The attendant or room that the event is assigned to.
Device MAC Address	The device's MAC address.
Attendant Name	The name of the attendant, if the event is assigned to an attendant.
Status	The action of the attendant. That is, whether the attendant in the Assigned To column acknowledged or declined the alert.
Time Added	The time of the alert.
Time Actioned	The time of the attendant's action.

11.7 Generating Summarized Archived Alerts Reports

The summarized archived alerts report displays a summary report for the events that you specify during the time that you specify. Each event is grouped by date and type. For example, if there are events for Patient Unit: Emergency Button, Pendant: Emergency Button, and Pull Station: Emergency Button, the summarized archived alerts report will group them together under the event type **Emergency Button**.

To generate a summarized archived alerts report:

- 1. From the Admin Portal, click Reports.
- 2. In the Archived Alerts Report section, click Summarized Archived Alerts Report.
- 3. Enter the start date and time and the end date and time for the report in the **Start** and **End** boxes.
 - You can either enter these values directly or click **Open the calendar** () to select a date and then click **Open the time view** () to select a time.
- 4. Select the filters for the report by unselecting the events that you do not want in the report. To not apply any filter(s), leave all the events selected.
 - Click the checkbox at the top of the list of events to unselect or select all the events at once.
- 5. Click Run Report.

The Summarized Archived Alerts Report displays at the bottom of the screen. For information on the report window (including how to save or print the report) see Section 11.8 on page 69.



11.8 The Report Window

Once a report is generated, you can navigate, zoom, search, save, refresh, or export the report. To perform these actions, click the appropriate icons on the report window toolbar.

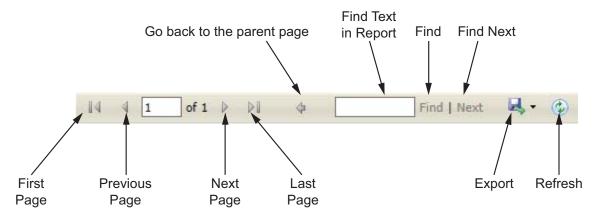


Figure 7 The report window toolbar

To download the report as an Excel, PDF, or Word document

1. Click **Export** button on the report window toolbar.

You can print the file after you have exported it.



12.0 Archived Alerts

The **Archived Alerts** page displays a log of all the alerts.

Table 2 Archived Alerts

Column	Description
Event	The type of event that triggered the alert. This includes a button press, or a low battery or technical fault.
Assigned To	The attendant, device, or room that the event is assigned to.
Attendant Name	The name of the attendant, if the event is assigned to an attendant.
Location	The location of the device.
Action	The action of the attendant. That is, whether the attendant in the Assigned To column acknowledged or declined the alert.
Device SN	The device's MAC address.
Event Time	The time of the alert.
Action Time	The time of the attendant's action.

To download the archived alerts as a CSV file for importing into Microsoft Excel

Click Download Archive File at the bottom of the page.



13.0 Network View

Network View lets you view the configuration of the wireless network.

The following topics are covered in this chapter:

- Network View
- Devices



13.1 Network View

To see the network view

- 1. From the Admin Portal, click Network View.
- 2. Select a building on the left.
- 3. Select a wing, and then select a floor.

A map of the floor appears, showing the wireless network configuration. Different networks appear as different colours.

- 4. Click a device in the map to see its information.
- 5. Click a device in the network tree on the right to see its information and location on the map.

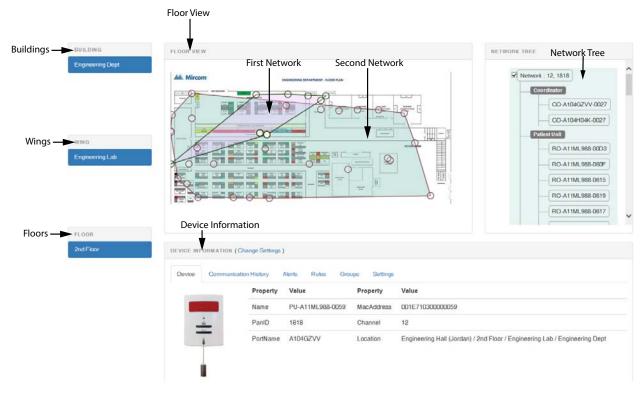


Figure 8 Network View

13.2 Devices

After you select a device, its information appears in the **Device Information** section at the bottom of the window.

- Device shows information about the device such as name and MAC address.
- Communication History shows the message that the device has sent and received.
- Alerts shows the alerts that have been initiated at the device.
- Rules shows the rules associated with the device. See Chapter 10.0.
- **Groups** shows the groups that the device is part of. See Chapter 9.0.
- **Settings** shows the device's settings. See Chapter 8.0.



14.0 The MiCare Processor

When messages are received at the Central server, they are handled by an application called the MiCare Processor. The Processor interprets each message and then decides what to do with it based on the settings and rules for the device that sent the message.

The following topics are covered in this chapter:

- Accessing the MiCare Processor
- Output Listing
- Notification Testing
- Settings
- Debug
- Monitoring



14.1 Accessing the MiCare Processor

The MiCare Processor runs on the Central server.

To access the MiCare Processor, log in to the computer that runs the Central server. You should see the MiCare Processor window (see Figure 9).

i

Note: If you do not see the MiCare Processor window, you have probably not logged in as the user running the MiCare Processor.

The MiCare Processor has five tabs:

- Output Listing
- Notification Testing
- Settings
- Debug
- Monitoring

Each of these tabs and what you can do in them are explained in sections 14.2 to 14.5. To access a tab, click on its label in the MiCare Processor window.

14.2 Output Listing

The Output Listing tab shows the processed messages the Processor has received from and sent to MiCare devices in the Nurse Call System. Each message entry shows the message date and time, the MAC address of the device that sent the message, the MAC address of the Coordinator that received the message, and a text description of the message (see Figure 9).

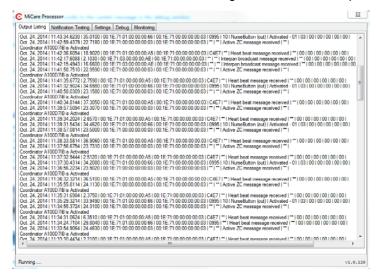


Figure 9 The Output Listing Tab



14.3 Notification Testing

You can simulate events on Nurse Call System with the Notification Testing tab (see Figure 10).

To simulate an event:

- 1. From the MiCare Processor, select the **Notification Testing** tab.
- 2. Select a device type from the **Device Type** list.
- 3. Select a device from the Device Id list.
- Select an event from the Event Type list.
- 5. If you are simulating a router, enter value between 1 and 4095 in the Ultrasonic Id box.
- Select a priority level for the event by moving the **Priority** slider.
- 7. Click Trigger.

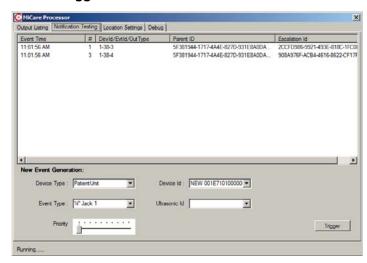


Figure 10 The Notification Testing tab

14.4 Settings

14.4.1 Discovery Mode

You must run Discovery Mode every time you make changes to the network (for instance, when you add a new device).

To run Discovery Mode

1. Choose either Single-storey Building (Triangulation) or Multi-storey Building (Trilateration).

Triangulation is more accurate for single-storey buildings as it is a 2-dimensional approach. Trilateration is more accurate for multi-storey buildings because it takes into account 3-dimensional space. If your site is a single-storey dwelling, select the **Single-storey Building (Triangulation)** option. If your site is a multi-storey dwelling, select the **Multi-storey Building (Trilateration)**.

Select a time in the **Timeout** menu. This is the number of minutes that you want discovery mode to be active.



3. Click Start.

Time Elapsed shows the number of seconds that discovery mode has been active.



Attention: The Advanced Settings should only be changed by Mircom service technicians. Changing the Advanced Settings could compromise the functioning of the Processor.

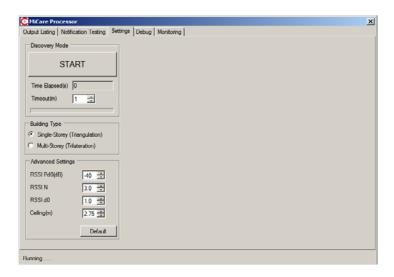


Figure 11 The Settings tab

14.5 Debug

The Debug tab shows all of the raw (hexadecimal) messages that the MiCare Processor receives and transmits (see Figure 12). Unlike the Output Listing tab, all messages are shown regardless of the quality of the messages. If, for example, a message cannot be interpreted because of poor reception, the message will not appear under the Output Listing tab but it will always appear under the Debug tab.

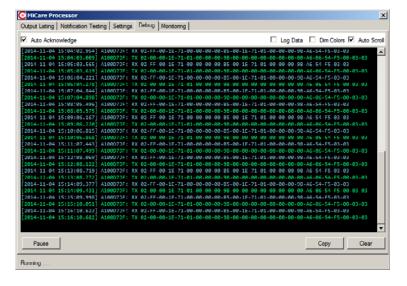


Figure 12 The Debug tab



The following is a list of the options and functions available for the Debug tab.

- Auto-acknowledge: This should be changed only by a Mircom service technician.
- Log Data: Select this option to automatically copy all messages as they are received by the MiCare Processor to a text file. For more information, see section 14.5.1, Logging Messages.
- Dim Colours: Select this option to reduce the brightness of the messages on the Debug screen.
- Auto-scroll: Select this option to automatically scroll to the current message.
- Pause: Temporarily stop messages from appearing on the screen. To start the messages, press Resume.
- Copy: Copy all of the messages in the Debug screen into the clipboard so they can be pasted into a text document.
- Clear: Delete all of the messages from the Debug screen.

14.5.1 Logging Messages

The Log Data option automatically saves all messages from the Debug screen to a text file.

To log debug messages to a text file:

- From the Debug tab, select the Log Data option.
 The MiCare Processor creates an log file and automatically saves debug messages to the debug file. To stop saving messages, clear the Log Data option.
- Browse to the folder that contains the MiCare Processor executable.
 If you do not know where the MiCare Processor executable is stored, find the MiCare Processor shortcut on your desktop (see the following figure), right click on the shortcut, and then select **Open file location**.



Figure 13 MiCare Processor Icon

3. Find the log file called **application**.

The **application** (or **application.log**) file contains all of the debug messages that have been received since you started logging data. It is a regular text file that can be opened in any text editor.

14.6 Monitoring

The Monitoring tab displays a list of the currently active coordinators.

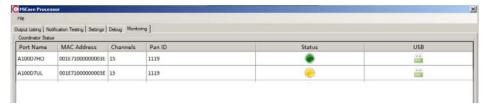


Figure 14 The Monitoring tab



15.0 Warranty and Warning Information

WARNING!

Please read this document **CAREFULLY**, as it contains important warnings, life-safety, and practical information about all products manufactured by the Mircom Group of Companies, including Mircom and Secutron branded products, which shall include without limitation all fire alarm, nurse call, building automation and access control and card access products (hereinafter individually or collectively, as applicable, referred to as "**Mircom System**").

NOTE TO ALL READERS:

- Nature of Warnings. The within warnings are communicated to the reader out of an abundance of caution and create no legal obligation for Mircom Group of Companies, whatsoever. Without limiting the generality of the foregoing, this document shall NOT be construed as in any way altering the rights and obligations of the parties, governed by the legal documents that apply in any given circumstance.
- 2. **Application.** The warnings contained in this document apply to all Mircom System and shall be read in conjunction with:
 - a. the product manual for the specific Mircom System that applies in given circumstances;
 - b. legal documents that apply to the purchase and sale of a Mircom System, which may include the company's standard terms and conditions and warranty statements;
 - c. other information about the Mircom System or the parties' rights and obligations as may be application to a given circumstance.
- 3. Security and Insurance. Regardless of its capabilities, no Mircom System is a substitute for property or life insurance. Nor is the system a substitute for property owners, renters, or other occupants to act prudently to prevent or minimize the harmful effects of an emergency situation. Building automation systems produced by the Mircom Group of Companies are not to be used as a fire, alarm, or life-safety system.

NOTE TO INSTALLERS:

All Mircom Systems have been carefully designed to be as effective as possible. However, there are circumstances where they may not provide protection. Some reasons for system failure include the following. As the only individual in contact with system users, please bring each item in this warning to the attention of the users of this Mircom System. Failure to properly inform system end-users of the circumstances in which the system might fail may result in over-reliance upon the system. As a result, it is imperative that you properly inform each customer for whom you install the system of the possible forms of failure:

- 4. Inadequate Installation. All Mircom Systems must be installed in accordance with all the applicable codes and standards in order to provide adequate protection. National standards require an inspection and approval to be conducted by the local authority having jurisdiction following the initial installation of the system and following any changes to the system. Such inspections ensure installation has been carried out properly.
- 5. **Inadequate Testing.** Most problems that would prevent an alarm a Mircom System from operating as intended can be discovered by regular testing and maintenance. The complete system should be tested by the local authority having jurisdiction immediately after a fire, storm, earthquake, accident, or any kind of construction activity inside or outside the premises.



The testing should include all sensing devices, keypads, consoles, alarm indicating devices and any other operational devices that are part of the system.

NOTE TO USERS:

All Mircom Systems have been carefully designed to be as effective as possible. However, there are circumstances where they may not provide protection. Some reasons for system failure include the following. The end user can minimize the occurrence of any of the following by proper training, testing and maintenance of the Mircom Systems:

- 6. Inadequate Testing and Maintenance. It is imperative that the systems be periodically tested and subjected to preventative maintenance. Best practices and local authority having jurisdiction determine the frequency and type of testing that is required at a minimum. Mircom System may not function properly, and the occurrence of other system failures identified below may not be minimized, if the periodic testing and maintenance of Mircom Systems is not completed with diligence and as required.
- 7. Improper Operation. It is important that all system users be trained in the correct operation of the alarm system and that they know how to respond when the system indicates an alarm. A Mircom System may not function as intended during an emergency situation where the user is unable to operate a panic or emergency switch by reason of permanent or temporary physical disability, inability to reach the device in time, unfamiliarity with the correct operation, or related circumstances.
- 8. **Insufficient Time.** There may be circumstances when a Mircom System will operate as intended, yet the occupants will not be protected from the emergency due to their inability to respond to the warnings in a timely manner. If the system is monitored, the response may not occur in time enough to protect the occupants or their belongings.
- 9. Carelessness or Safety Hazards. Moreover, smoke detectors may not provide timely warning of fires caused by carelessness or safety hazards such as smoking in bed, violent explosions, escaping gas, improper storage of flammable materials, overloaded electrical circuits or children playing with matches or arson.
- 10. Power Failure. Some Mircom System components require adequate electrical power supply to operate. Examples include: smoke detectors, beacons, HVAC, and lighting controllers. If a device operates only by AC power, any interruption, however brief, will render that device inoperative while it does not have power. Power interruptions of any length are often accompanied by voltage fluctuations which may damage Mircom Systems or other electronic equipment. After a power interruption has occurred, immediately conduct a complete system test to ensure that the system operates as intended.
- 11. Battery Failure. If the Mircom System or any device connected to the system operates from batteries it is possible for the batteries to fail. Even if the batteries have not failed, they must be fully charged, in good condition, and installed correctly. Some Mircom Systems use replaceable batteries, which have a limited life-span. The expected battery life is variable and in part dependent on the device environment, usage and type. Ambient conditions such as high humidity, high or low temperatures, or large temperature fluctuations may reduce the expected battery life. Moreover, some Mircom Systems do not have a battery monitor that would alert the user in the event that the battery is nearing its end of life. Regular testing and replacements are vital for ensuring that the batteries function as expected, whether or not a device has a low-battery monitor.
- 12. Physical Obstructions. Motion sensors that are part of a Mircom System must be kept clear of any obstacles which impede the sensors' ability to detect movement. Signals being communicated by a Mircom System may not reach the receiver if an item (such as metal, water, or concrete) is placed on or near the radio path. Deliberate jamming or other inadvertent radio signal interference can also negatively affect system operation.



- 13. Wireless Devices Placement Proximity. Moreover all wireless devices must be a minimum and maximum distance away from large metal objects, such as refrigerators. You are required to consult the specific Mircom System manual and application guide for any maximum distances required between devices and suggested placement of wireless devices for optimal functioning.
- 14. **Failure to Trigger Sensors.** Moreover, Mircom Systems may fail to operate as intended if motion, heat, or smoke sensors are not triggered.
 - a. Sensors in a fire system may fail to be triggered when the fire is in a chimney, walls, roof, or on the other side of closed doors. Smoke and heat detectors may not detect smoke or heat from fires on another level of the residence or building. In this situation the control panel may not alert occupants of a fire.
 - b. Sensors in a nurse call system may fail to be triggered when movement is occurring outside of the motion sensors' range. For example, if movement is occurring on the other side of closed doors or on another level of the residence or building the motion detector may not be triggered. In this situation the central controller may not register an alarm signal.
- 15. **Interference with Audible Notification Appliances.** Audible notification appliances may be interfered with by other noise sources such as stereos, radios, televisions, air conditioners, appliances, or passing traffic. Audible notification appliances, however loud, may not be heard by a hearing-impaired person.
- 16. **Other Impairments.** Alarm notification appliances such as sirens, bells, horns, or strobes may not warn or waken a sleeping occupant if there is an intervening wall or door. It is less likely that the occupants will be alerted or awakened when notification appliances are located on a different level of the residence or premise.
- 17. **Software Malfunction.** Most Mircom Systems contain software. No warranties are provided as to the software components of any products or stand-alone software products within a Mircom System. For a full statement of the warranties and exclusions and limitations of liability please refer to the company's standard Terms and Conditions and Warranties.
- 18. **Telephone Lines Malfunction.** Telephone service can cause system failure where telephone lines are relied upon by a Mircom System. Alarms and information coming from a Mircom System may not be transmitted if a phone line is out of service or busy for a certain period of time. Alarms and information may not be transmitted where telephone lines have been compromised by criminal tampering, local construction, storms or earthquakes.
- 19. Component Failure. Although every effort has been made to make this Mircom System as reliable as possible, the system may fail to function as intended due to the failure of a component.
- 20. Integrated Products. Mircom System might not function as intended if it is connected to a non-Mircom product or to a Mircom product that is deemed non-compatible with a particular Mircom System. A list of compatible products can be requested and obtained.

Warranty

Purchase of all Mircom products is governed by:

https://www.mircom.com/product-warranty

https://www.mircom.com/purchase-terms-and-conditions

https://www.mircom.com/software-license-terms-and-conditions

