



User Manual

December 2000

March 2000, Revision 5.0, Added FCC Regulations
December 2000, Revision 6.0, Added new features from HALO™ software version 3.1

© Copyright 2000, EXI Wireless Systems Inc., All rights reserved.

Revision 6.0

Table of Contents

<u>ABOUT THIS DOCUMENT</u>	3
<u>1. SYSTEM INTRODUCTION</u>	5
1.1. <u>SYSTEM COMPONENTS</u>	5
1.2. <u>TERMS USED IN THIS DOCUMENT</u>	5
1.3. <u>COMPUTER DISPLAY CONVENTIONS</u>	6
<u>2. USER LEVEL FUNCTIONS</u>	8
2.1. <u>ADMITTING A PATIENT</u>	8
2.2. <u>DISCHARGING OR EDITING A PATIENT</u>	11
2.3. <u>DISABLING A TAG TEMPORARILY</u>	13
2.4. <u>SILENCING AND ACCEPTING ALARMS</u>	15
2.5. <u>“NURSE SAVER” AND “LOITERING” FEATURES</u>	17
2.6. <u>IMPROPERLY STORED TAGS</u>	17
<u>3. SUPERVISOR LEVEL FUNCTIONS</u>	19
3.1. <u>ACCESSING SUPERVISOR LEVEL</u>	19
3.2. <u>EXITING SUPERVISOR LEVEL</u>	20
<u>4. ACTIVITY LOG MANAGEMENT</u>	21
4.1. <u>ACTIVITY LOGS</u>	21
4.2. <u>NAVIGATING THE ACTIVITY LOG</u>	22
4.3. <u>ADDING A SUPERVISOR ANNOTATION TO AN ALARM</u>	22
4.4. <u>BACKING UP ACTIVITY LOGS</u>	23
<u>5. MANAGING TAGS</u>	24
5.1. <u>TAGS</u>	24
5.2. <u>ADDING A NEW P-TAG TO THE SYSTEM</u>	25
5.3. <u>DELETING A P-TAG FROM THE SYSTEM</u>	26
5.4. <u>DISABLING A P-TAG</u>	27
5.5. <u>UNASSIGNING A P-TAG</u>	27
5.6. <u>EDITING A P-TAG RECORD</u>	28
5.7. <u>CHANGING A TAG’S EXPIRY DATE</u>	28
5.8. <u>LOCATE A TAG</u>	29
<u>6. MANAGING SYSTEM USERS</u>	30
6.1. <u>ADDING A NEW USER TO THE SYSTEM</u>	31
6.2. <u>DELETING A USER FROM THE SYSTEM</u>	32
6.3. <u>DISABLING A SYSTEM USER</u>	32
6.4. <u>EDITING A SYSTEM USER’S ACCESS LEVEL</u>	32
<u>7. PRINTING LOGS</u>	33
<u>8. MANAGING ALARM ANNOTATIONS</u>	34
8.1. <u>ADDING AN ANNOTATION</u>	35
8.2. <u>DELETING AN ANNOTATION</u>	35
8.3. <u>EDITING AN ANNOTATION</u>	35
<u>9. SHUTTING DOWN AND RESTARTING THE SYSTEM</u>	36
9.1. <u>SHUTTING DOWN</u>	36
9.2. <u>RESTARTING THE SYSTEM</u>	36
<u>APPENDIX A - LIMITED WARRANTY</u>	37
<u>APPENDIX B - FCC REGULATIONS</u>	38
<u>APPENDIX C - SYSTEM MAINTENANCE</u>	39

ABOUT THIS DOCUMENT

Intended Audience

This manual is intended for system users (typically duty nurses), team leaders, and supervisory level users who manage the system and the system users.

Scope

This manual will provide step-by-step instructions for users and supervisors who administer the usage of the system. The HALO™ system features a very simple user interface that guides the user through each step.

About the Halo Infant Protection System

- HALO™ is a premium infant protection system.
- HALO™ works in conjunction with the EXI P-tag patient transponder that is capable of sensing if it has been removed from the infant.
- HALO™ is an electronic system, which, in conjunction with staff diligence, creates a secure perimeter to deter infant abductions.
- HALO™ will detect if an infant is near a controlled exit and invoke countermeasures.
- The system will identify the infant, the location and the time.
- Alarms must be accepted by staff using password access to the system.
- The system maintains a log of all activity.

Access Levels

The HALO™ system has three separate access levels:

- User
- Team Leader
- Supervisor

Level	Password required	Functions	Access Management
User	Yes	Admit Patients Discharge Patients Accept/Silence alarms Toggle between floor plans	Access controlled by Supervisor level users
Team Leader	Yes	All user functions Temporarily Disable Patient	Access controlled by Supervisor level users

Supervisor	Yes	All team leader functions Manage user list Assign usernames and passwords View and annotate activity logs Add/Delete tags from fleet Add alarm annotations Initiate System Data Backups Print logs Exit the HALO™ system	The first Supervisor is setup by the installing dealer. This Supervisor may add more assigned supervisory access.
------------	-----	--	---

System Conventions

Each user in the system has a unique identity (username) and password. The Supervisor assigns both the username and password. It is suggested that both be kept between 4-8 characters to provide sufficient security and allow users to easily enter and remember their system access codes. For example: a user named Barbara Smith would have a username such as bsmith or barbs. Note that that each user must have a unique name.

The system prompts the user for any text entry such as usernames or infant names, etc. To move from one field to the next, the user may press Tab key on the keyboard or place the mouse cursor over the field and Click the left button.

System Support

For system service or support contact your installing dealer

Or contact:

EXI Wireless Systems Inc.
Suite 100-13551 Commerce Parkway
Richmond, BC V6V 2L1
Canada
Ph: 1-800-667-9689
Fax: 604-207-7760
Website: www.exi.com

1. SYSTEM INTRODUCTION

1.1. System Components

HALO™ Software: Primary user interface that assists in the assignment and tracking of Transponders, and displays alarms and other activities in graphical format. It also stores and allows printing of all system events that have been logged.

Controllers: Controls an egress point and reports any Tag presence at the egress point to the computer. Depending on system configuration, controllers may control door locks and local alarms, and allow keypad input for door bypass. They may also provide a “Nurse Saver” and “Loiter” feature. The “Nurse Saver” feature eliminates nuisance alarms by not setting off an alarm when the presence of a Tag is detected and the door is sensed as closed. In the event that the door is open, or is opened when the Tag is at the egress point, the system will alarm. The “Loiter” feature sounds an alarm if a Tag detected at a door remains at that door for a period of time, regardless of the fact that the door may be sensed as closed.

Controllers will also detect a “Tag off body” condition in its area, as does a Receiver.

Receivers: Detects “Tag off body” condition when a Tag is removed from a patient, and reports this activity to the computer.

Transponders: Also referred to as “Tags”, these devices are attached to the patient. Tags initiate two different kinds of alarm conditions as follows:

TIC - Tag-initiated-Communications:

This alarm is initiated in the event that a Tag is removed from a patient. This occurs when the Tag can no longer sense the body of the patient.

TIF - Tag-in-field Communications:

This alarm is initiated when a Tag enters an area protected by a Controller. The Controller’s antenna(s) emit a constant field of radio waves that is picked up by the Tag when in the proximity of the Controller. The Tag reports its presence to the Controller, and therefore the system, when it senses this field of radio waves.

1.2. Terms used in this document

The following terms are used to help explain user functions in this document:

- **Press** means to press a key on the keyboard

- **Click** means click the left mouse button once. This term is usually used for an action button, for example, to complete a function place the mouse pointer over the button then click the left mouse button.

- **Select** means you position the mouse pointer in a data area and click the left mouse button. This term is usually used to highlight data, for example when that data is to be changed, or deleted..

- Θ Names of keys are shown as the physical keys on a keyboard.

-  Names of dialog boxes, screens, and field titles in forms are bolded or shown graphically.
-  Names of buttons are shown as on screen.

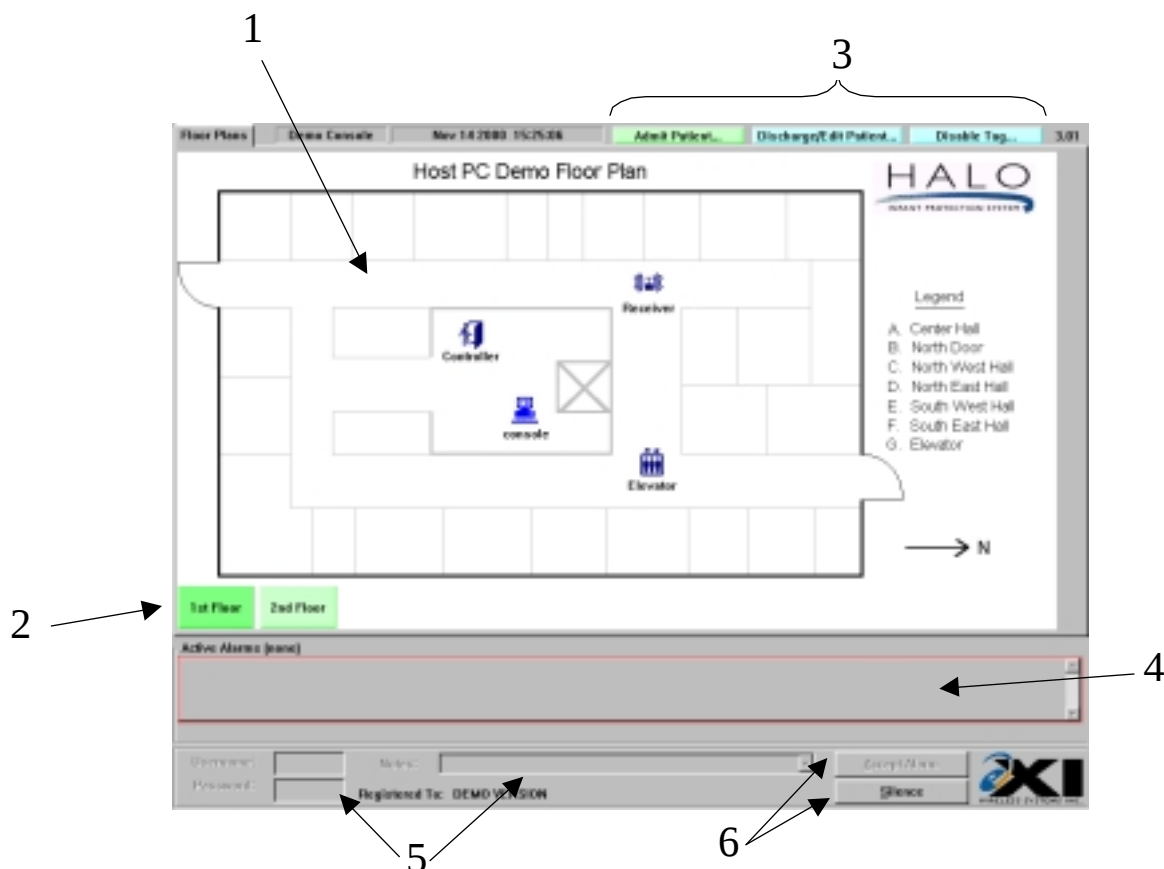
1.3. Computer Display Conventions

The computer displays various types of information, which is color-coded, to differentiate between the Supervisor and User modes. In addition, the “Icons” that display the locations of the various system components such as the Controllers and the Receivers, and the on-screen “buttons” may also change color to indicate their status.

The table below shows the various icons, and alarm conditions.

Icon	Name	Description
	Controllers	The controllers are located near egress points, such as doors. This icon will flash red if there is a communication problem.
	Receivers	Receivers can be placed anywhere, and will only detect off-body TIC alarms.
	Elevators	Elevators are controllers which detect TIC or TIF alarms near an elevator.
	Console	The console is the computer that runs the HALO™ software.
	Pre-alarm	
	Alarm Condition	Controllers or Receivers will flash these two icons when they receive a TIC, a TIF, or a loiter alarm.
		

The figure below shows a typical user screen and identifies its components.



Walk around:

1. This is the floor plan area. It shows the positions of all controllers, receivers, elevators, and consoles that are installed in your system.
2. Floor navigation buttons. Clicking on the desired floor will cause that floor to be displayed on the screen. The buttons will change color depending on the alarms have occurred on each floor:-
Green: Normal
Blue: Indicates that the cursor is positioned over button
Yellow: Indicates Pre-alarm condition on floor
Red: Alarm condition on this floor
3. These are the action buttons. From here you can **Admit a Patient** and **Discharge or Edit a Patient**. Team leaders may also **Disable a Tag**.
4. This is the list of **Active Alarms**. When an alarm occurs, the description of the alarm will be displayed in this window. In order to **Silence** or **Accept the Alarm**, you must point the mouse to the line with alarm, and click the left mouse button to select. When the alarm is selected it will turn blue.
5. Once an alarm has been selected from the **Active Alarms** list, the **Username**, **Password**, and **Notes** fields will become active. In order to accept an alarm, these three fields must be filled in.
6. These are the **Accept Alarm** and **Silence** buttons. Once the **Username**, **Password**, and **Notes** fields are filled in, the **Accept Alarm** button will become active. Click on the **Accept Alarm** button to accept the alarm. The **Silence** button is always available after selecting an alarm from the list.

2. USER LEVEL FUNCTIONS

The Halo system provides a simple, intuitive user interface. After each step, the system will automatically take you to the next step until the task is complete.

2.1. Admitting a Patient

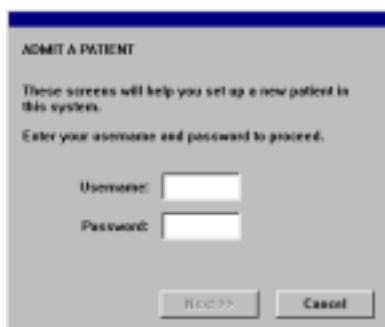
Select the **Admit Patient...** button on the top right of the screen.



Main Screen - User Level

Enter Username and Password:

1. Type in your **Username** as assigned by your supervisor.

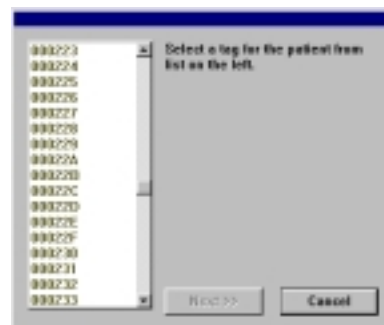


2. Press the **⏏** key on the keyboard
3. Type in your **Password**
4. Press the **⏏** key on the keyboard, or click on the **Next >>** button.
5. The **Select a tag** screen will appear.

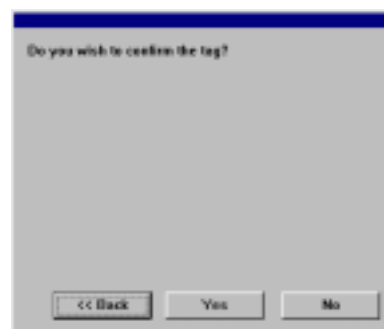


Select a Tag:

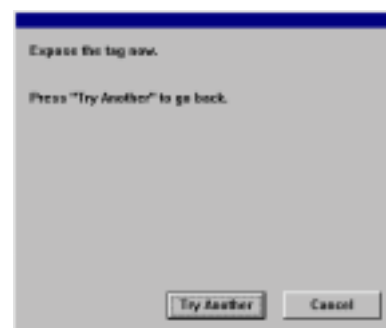
1. Select the tag number that corresponds to the serial number on the side of the tag you wish to use. The list contains only available tags which have been registered in the system but not assigned to an infant.
2. Click on  to go to the **Confirm Tag** step.

**Confirm Tag:**

1. Click on  to begin a test of the tag.
 - We recommend that you test each tag before use. The system will guide you through the process

**Test tag**

1. Expose the tag, or trigger an off-body TIC alarm
 - During this test, the system is
 - verifying the tag serial number
 - testing the tag removal alarm
 - generating an activity log entry to document the test.



If the test is successful, the system will take you to the next step in the admit process.

If the controller cannot detect the tag, select  to go back and try another tag.

Ensure the bottom of the tag is held stable on your skin during the test for about 10 seconds prior to removing.

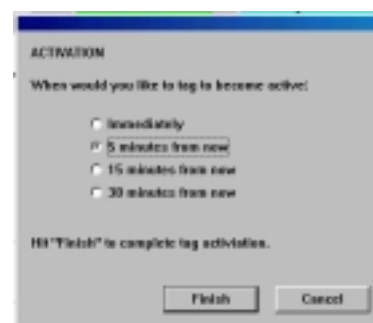
If the test fails, try it once more on your wrist.

Enter Patient Information:

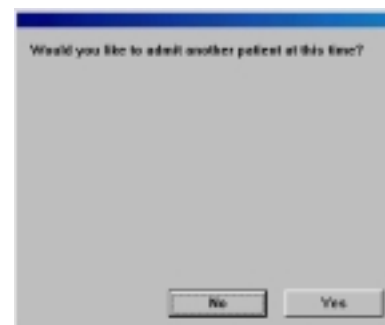
1. Verify that the **Tag #** shown matches the serial number on the Tag you have just selected
2. Type the **Patient info**
3. Click  when done.

**Choose Activation Delay:**

1. Select the required **Activation** delay
2. Click on  to complete the admission
3. NOTE that Delays apply to sensing “off- body” or TIC alarms only. Tag will still initiate alarms at egress points.

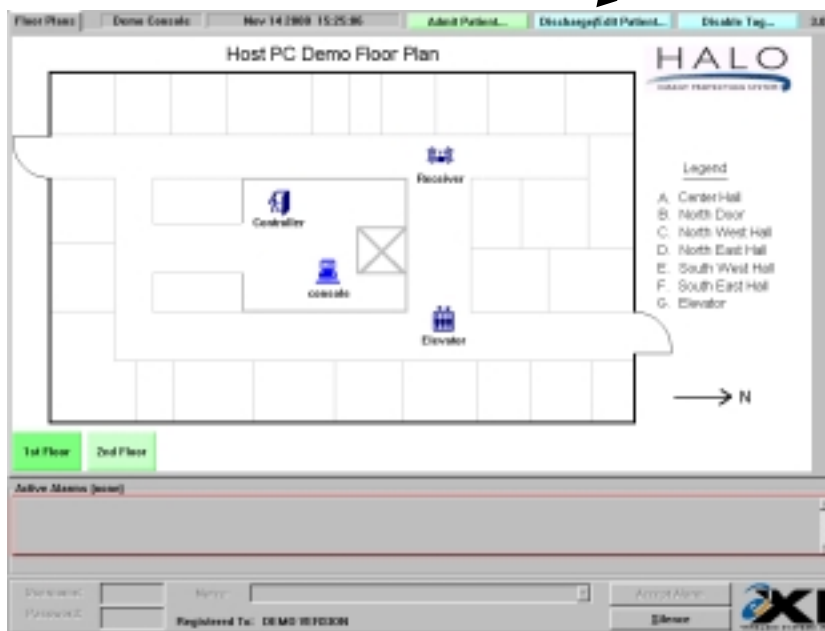


1. Click on  to admit another patient
2. Click on  to return to the main screen



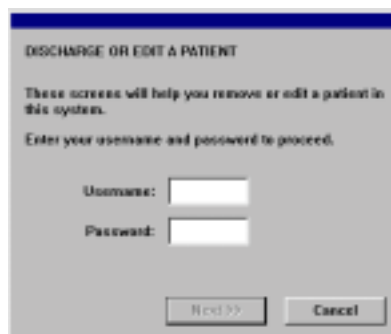
2.2. Discharging or Editing a Patient

Select the **Discharge/Edit Patient...** button on the top right of the screen.



Main Screen - User Level

Enter Username and Password:

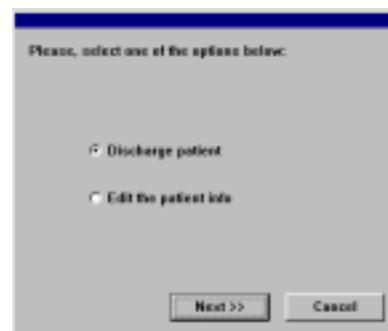


1. Type in your **Username** as assigned by your supervisor.
2. Press the $\ominus$ key on the keyboard
3. Type in your **Password**
4. Press the $\equiv$ key on the keyboard, or click on the **Next >>** button.

Next >>

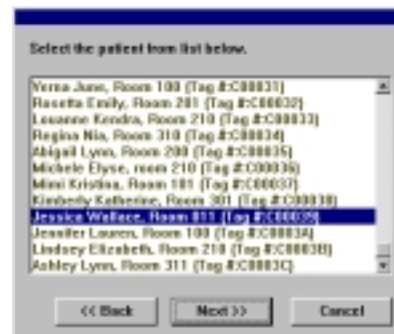
Select Option

1. Select the option require.
2. Click on



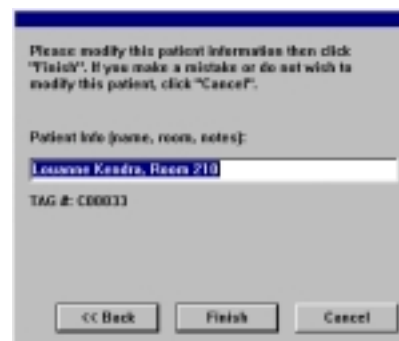
Select Patient:

1. Select the **Patient Name/Tag** that you wish to either discharge or edit
2. Click on .



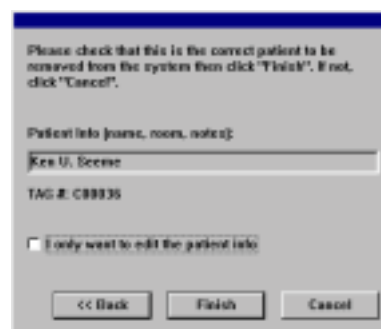
Editing a Patient's Info:

1. Type the changes to the existing information
2. Click on .



Discharging a Patient:

1. Verify the **Infant Name**
2. Click on  to discharge the infant
3. Click on  or  if the infant is not to be discharged.
4. Note: The system will continue to respond to a tag detected at an egress point, such as a doorway or elevator, and control that egress point even after the tag has been discharged.



2.3. Disabling a Tag Temporarily

The newest version of the HALO™ software allows a user with **Team Leader** or **Supervisor** access to temporarily disable a tag for a period of 5, 10 or 15 minutes.

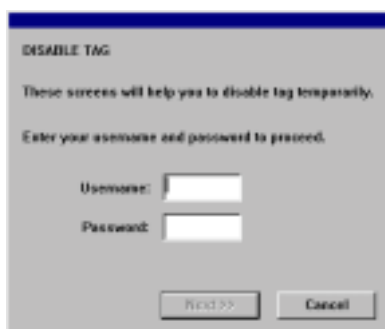
To temporarily disable a P-Tag from the console:

Select the **Disable Tag...** button on the top-right hand corner of the console.



Main Screen - User Level

Enter username and password:

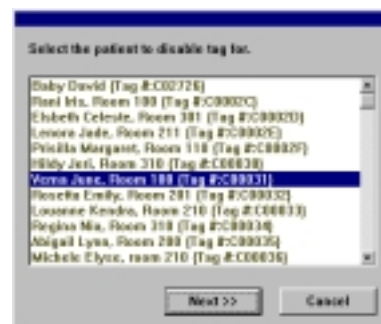


1. Type in your **Username** as assigned by your supervisor.
2. Press the **⌫** key on the keyboard
3. Type in your **Password**
4. Press the **⏎** key on the keyboard, or click on the **Next >>** button.

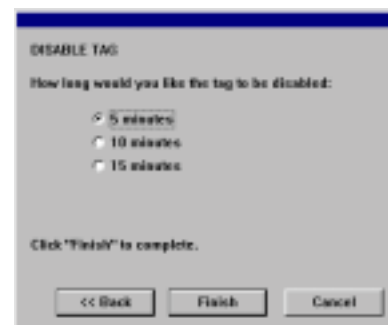


Select patient:

1. Select the patient whose tag you wish to disable
2. Click on press the  button.

**Choose time delay:**

1. Select the length of time the tag is to be disabled for
 2. Click on 
- Choose the minimum time that you think is necessary
 - The Disable Tag feature accessible from the Control Panel only
 - Only off-body (TIC) alarms are delayed for the selected amount of time.
 - TIF alarms, created when a tag is near an egress point can still be triggered during this period.



Click on  to disable another tag

Click on  to return to the main screen



2.4. Silencing and Accepting Alarms

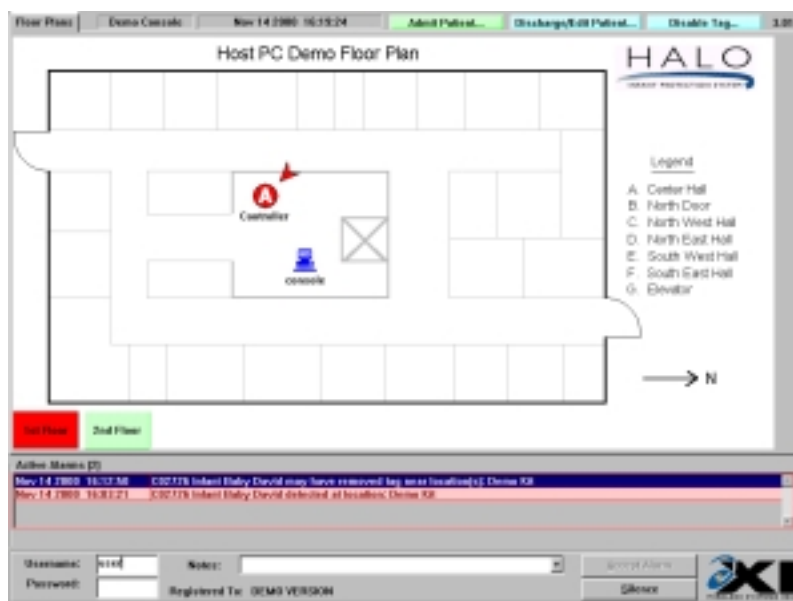
The HALO™ system will cause an alarm when:

- An assigned infant tag has been removed from an infant (off-body or TIC).
- When an infant tag is detected near a controlled egress area (in-field or TIF).

When an alarm occurs, the Alarm Acceptance Area will appear and the system will:

- Identify the infant associated with the detected tag.
- Identify the location by flashing an icon and expressing the location name.
- Identify the alarm type as a tag removal or egress area detection.
- Sound an audible alarm at the computer.

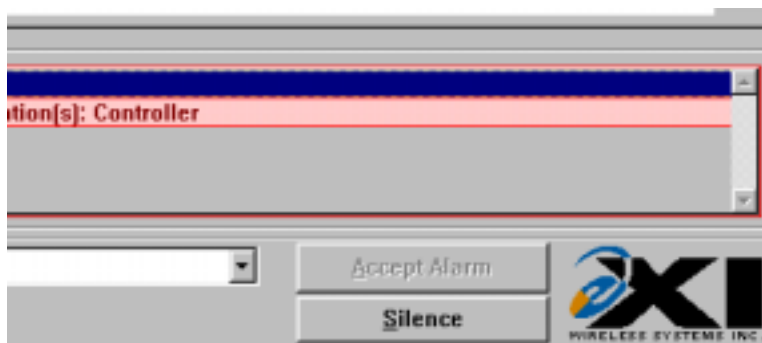
When multiple system devices see the same tag in alarm, the system will condense them into one incident. However, each alarm must be Accepted individually.



Alarm
Acceptance
Area

Main Screen - User Level

Silencing an alarm



1. Click on 
- After the alarm has been investigated you must Accept it.

Accepting an alarm

- Select the alarm condition in the **Active Alarms** field. If only one alarm exists, it will automatically be selected.

1. Type in your **Username**
2. Press the  key.
3. Type in your **Password**
4. Press the  key.



5. Enter a note in the **Notes** field You may not proceed until a Note has been entered
 - by typing from the keyboard
 - or
 - selecting a pre-defined note from the drop down list. Use the up and down arrows to find the note you want, and then select that note
6. Click on 

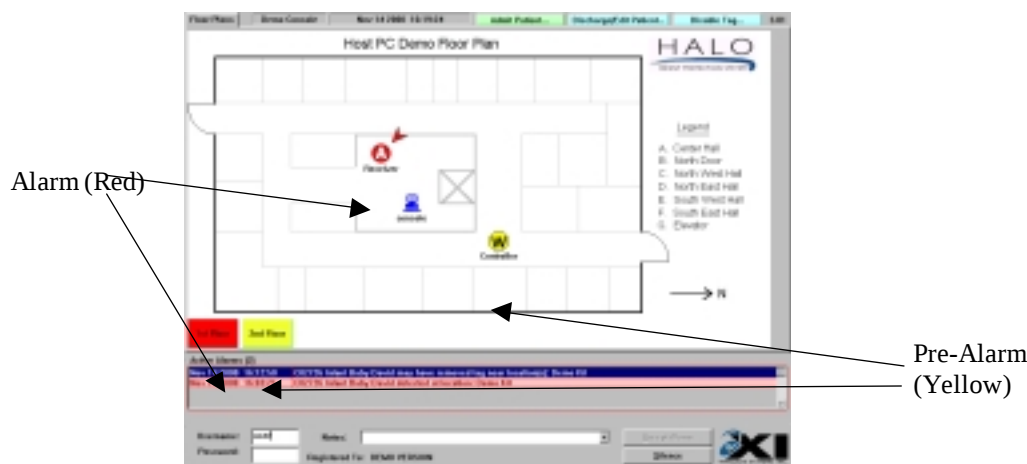


The system will log the following incident details:

- Alarm type (tag removal or egress alarm)
- Infant name
- Tag number
- Time
- ID of staff member accepting the alarm
- Staff member notes on alarm incident

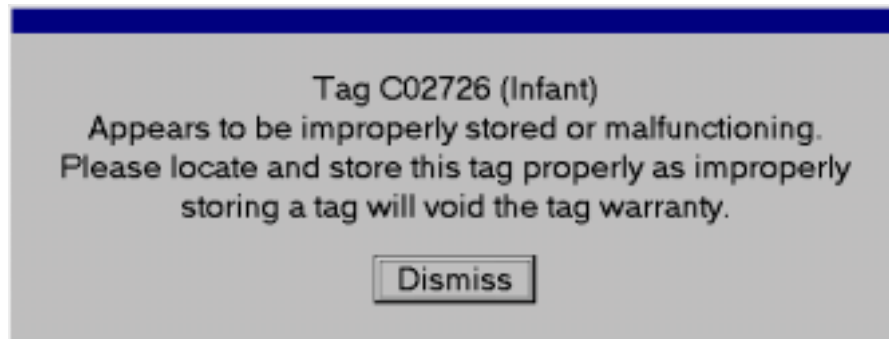
2.5. “Nurse Saver” and “Loitering” Features

- If the system is installed with the “Nurse Saver” feature, Tags detected at egress points that are secured will not set off nuisance alarms.
- A Tag detected near a door that is closed will result in the appropriate floor button on the computer screen turning yellow (pre-alarm), and the icon associated with that door also turning yellow.
- If a bypass keypad is installed at the door, it will flash a light and emit periodic “beeps” to indicate the presence of the Tag. This event is logged into the computer as “Tag detected at location xxx”, but will not create an alarm condition.
- If the door is opened while the Tag is still near the door an alarm will be initiated. This feature can only operate if the door is equipped with a magnetic switch to sense whether it is open or closed.
- If the tag remains near the door for a period of one minute or more, an egress alarm will be initiated and the button and the icon on the screen will both turn to red. This is the “Loitering” feature.



2.6. Improperly Stored Tags

- When a tag generates 20 or more off-body (TIC) alarms in a 24-hour period this usually means that the tag is improperly stored.
- When this occurs, a warning message will be displayed on the screen.



1. Note the Tag number
2. Follow the Instructions in the Warning Message
3. When you have read the message, click the  button.

- It is recommended that you attempt to locate the tag after the above message is given.
- Improperly storing a tag will void the tag warranty

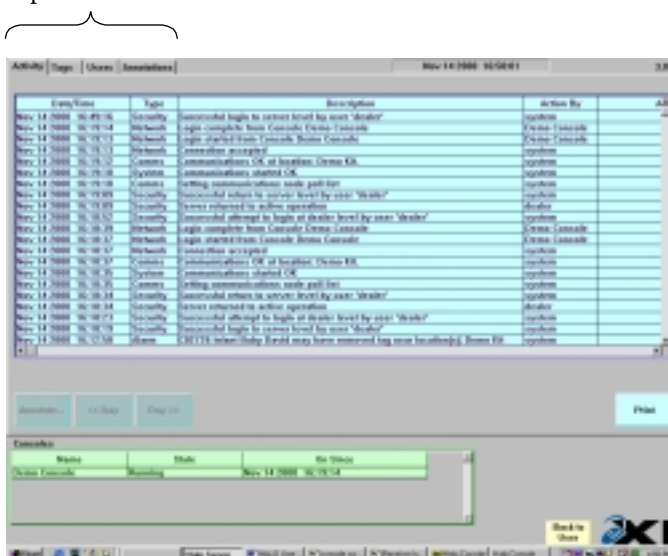
3. SUPERVISOR LEVEL FUNCTIONS

3.1. Accessing Supervisor Level

1. Hold the **Ξ** down, and press the **Θ** key.
2. Enter your **Username**
3. Press the **Θ** key on the keyboard
4. Enter your **Password**
5. Click on **OK** the Supervisor screen will appear - as shown below.



Supervisor Tabs



Supervisor's Screen

Supervisor mode has four different functions, each of which can be accessed from one of the four supervisor tabs shown in the figure above. There are:

- Activity
- Tags
- Users
- Annotations

Supervisor Level Functions

Supervisor tab	Access	Functions
Activity	Supervisor only	View activity logs Annotate activity logs Print logs
Tags	Supervisor only	Add or delete tags View registered tag list Disable a tag Unassign a tag Edit patient information for tag View current infant population Change expiry date of tags Locate a tag Print list of tags
Users	Supervisor only	Add or delete a user Disable or Activate a user Change user passwords
Annotations	Supervisor only	Add or delete alarm annotations Edit an annotation

3.2. Exiting Supervisor Level

Click on the  button at the bottom of the screen.

4. ACTIVITY LOG MANAGEMENT

4.1. Activity Logs

The system gives supervisors the ability to search the historical activity log. The system will record:

- Patient admission and discharge
- Alarm events including acceptance parameters
- System diagnostics
- Entry and Deletion of new tags and users
- Warning of unassigned tags or tags not in the database
- Door bypass activity

From the Supervisor Screen

Click on the Supervisor function tab



Activity Screen - Supervisor Level

The activity log screen will display:

- The time and day of activity
- The type of activity
- Description of the activity
- The user name associated with the activity
- The user notes.

4.2. Navigating the activity log

To look at an activity event on a specific day find the day using the “Day” buttons.

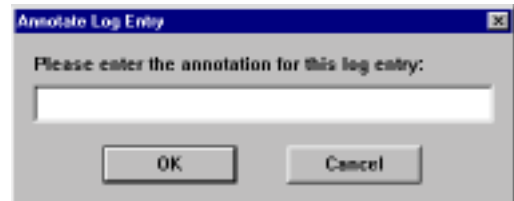
To step one day back, click on 

To step one day forward, click on 

The date you are viewing will appear in the leftmost column.

4.3. Adding a Supervisor annotation to an alarm

1. Select the particular alarm you wish to annotate.
2. Click on the Supervisor tab labeled 
3. Enter the note
4. Select  to accept, or  to cancel



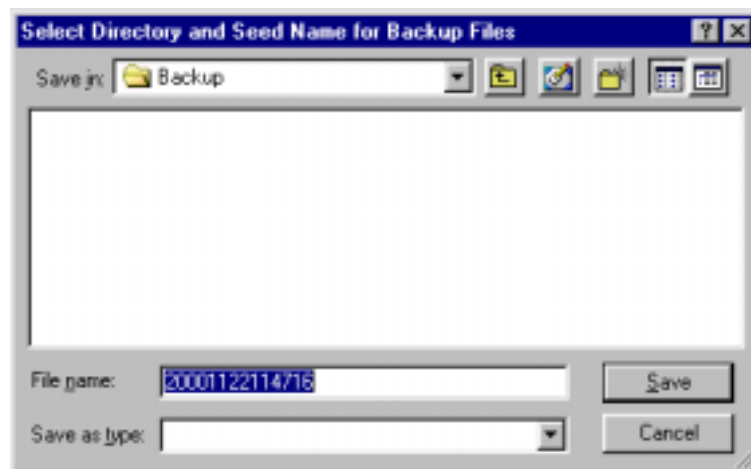
4.4. Backing up Activity Logs

For security and audit purpose we recommend that you copy the Activity Logs on a regular basis. The system is capable of storing 14,000 events in the Activity Logs. After the 14,000 events are captured, subsequent events displace the first log in the list. That is, events are purged on a first-in first-out basis after the 14,000 limit is reached.

Remember that all system activities, including alarm conditions, pre-alarm conditions, door access and bypass activities are logged.

To make a copy, or back-up, file of an Activity Log on the computer Hard Drive

1. you must be in Supervisor mode — see section 3.
2. Simultaneously press the Ξ and β keys on the Keyboard.
3. A window will appear, asking you to specify the filename and directory for the backup file storage. This window contains the default directory “Backup” and the default file name of the year, month, date, hour, minutes, and seconds when the backup was initiated. You can type in your own file name, or use the default. Click on the  save the backup file to the hard drive, or press  el the backup operation.



4. To access the back-up file look in the HALO™ directory using Windows Explorer

To make copies of these files for archiving, you will need to exit the HALO™ Console application and manually copy the back-up file to the removable back-up media (such as a ZIP Disk) using the Windows Explorer program.

5. MANAGING TAGS

5.1. Tags

Your system requires each infant to wear a P-Tag. You should have a fleet of tags on hand that exceeds your peak demand. Each tag has a unique serial number that is on the side of the tag.

The tag management tab allows a Supervisor to:

- Add new tags to the system.
- Delete tags from the system.
- View the existing tag fleet and edit the properties of each.
- Disable or Unassign a tag.
- Edit patient information for an assigned tag.
- Print the list of tags in the fleet.
- Change a tag's expiry date.
- Locate a tag.
- Print the tag listing.

To manage tags, you must be in the Supervisor mode – see Section 3.

- Click on the Supervisor tab labeled **Tags**



Tags Management Screen - Supervisor Level

5.2. Adding a new P-Tag to the system

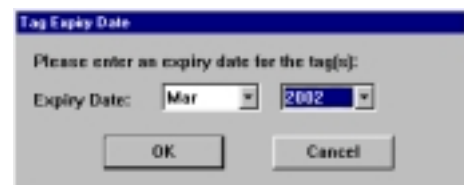
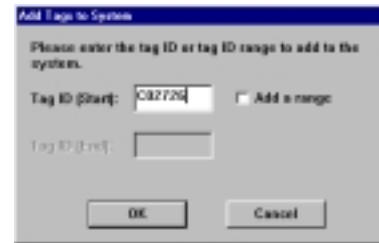
To add a new P-Tag to the system, you must be at the **Tags Management Screen**

P-Tags may be added to the system manually from the console, or by using the HALO™ network to read them.

When a number of Tags are to be added we suggest that you use the HALO™ network

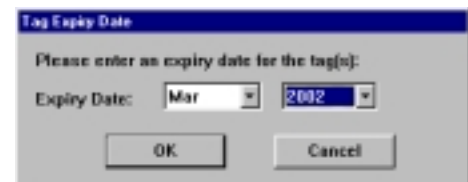
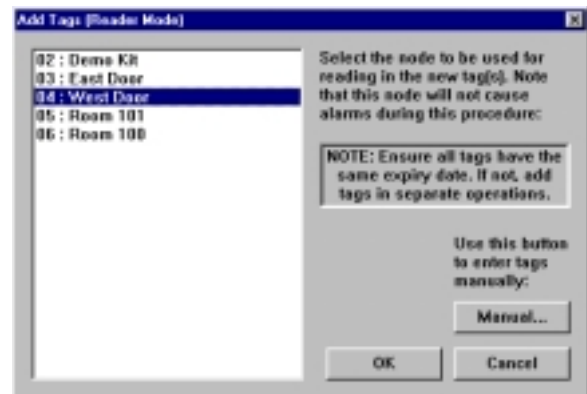
To add manually:

1. Click on **Add...** on **Tag Management Screen**
2. Click on **Manual...**
3. Enter the serial number in the **Tag ID (Start)** field.
4. If you wish to enter a *Range* of tags, click the ☐ **Add a range** button, if not skip to step 6.
5. Enter the **Starting ID** and the **End ID**.
6. Enter the tag **Expiry Date** either by keying the month and year or selecting from the menus using the drop-down arrows.
7. Select **OK**



To use the HALO™ network to read the tags in:

1. Select **Add...**
2. Select the device you wish to use to read the tags
3. Click on **OK**
 - The device will be **Reader Mode**
 - Note – a device in Reader Mode is not available for normal alarms
4. Enter the tag expiry date either by keying the month and year or selecting from the menus using the drop-down arrows.
5. Wave the tag in the air ensuring you are not contacting the bottom of the tag. The HALO™ software will read the tag in to the system automatically.
6. Exit Reader Mode by clicking on the **Clear Reader Mode** button.



- It is important to **Clear Reader Mode** to ensure that the device comes back on line and is ready to report alarms.

5.3. Deleting a P-Tag from the system

To delete a P-Tag, you must be at the **Tags Management Screen**



Tags Management Screen - Supervisor Level

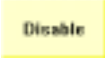
To delete a tag:

1. Select the tag to be deleted
2. Click on  button.

5.4. Disabling a P-Tag

- Disabling a tag can now be done from the console screen or from the supervisor level.
- Tag disabling allows for removal of the tag from the infant without triggering an alarm. The infant is not discharged from the system.
- Once you have disabled the tag you are responsible to enable it again or remove the infant from the system.
- This event is captured in the Activity log.

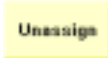
To disable a P-Tag

1. Select the tag to be disabled
2. Click on 

5.5. Unassigning a P-Tag

- P-Tags can only be unassigned from the **Tags Management Screen**
- The patient's name will be removed from the system when the tag is unassigned.

To unassign a tag:

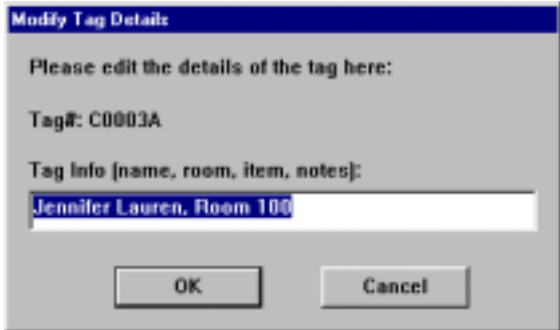
1. Select the tag to unassign
2. Click on 

5.6. Editing a P-Tag Record

- P-Tags can only be edited from the **Tags Management Screen** in Supervisor level.
- Only P-Tags assigned to a patient may be edited.
- The edit function allows a Supervisor to edit the **Tag info** associated with the tag serial number

To edit a P-Tag record

1. Select the tag to be edited
2. Click on 
3. Enter the required details in the **Tag info** field
4. Click on  to accept changes,  to undo changes.

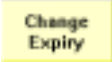


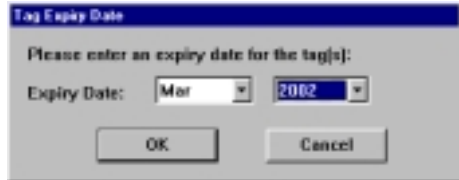
The dialog box is titled "Modify Tag Details". It contains the text "Please edit the details of the tag here:". Below this, it shows "Tag#: C0003A". Under "Tag Info (name, room, item, notes):", there is a text field containing "Jennifer Lauren, Room 100". At the bottom, there are "OK" and "Cancel" buttons.

5.7. Changing a Tag's Expiry Date

- P-Tags Expiry dates can only be changed from the **Tags Management Screen**
- This feature should be used with extreme caution
- The tag's expiry date is an important safety feature, which is meant to prevent tags which have old batteries from being used in the field.

To change a tag's expiry date

1. Select the tag on the **Tags Management Screen**
2. Click on 
3. Enter the tag **Expiry Date** either by keying the month and year or selecting from the menus using the drop-down arrows.
4. Click on  to accept change,  to abandon change.



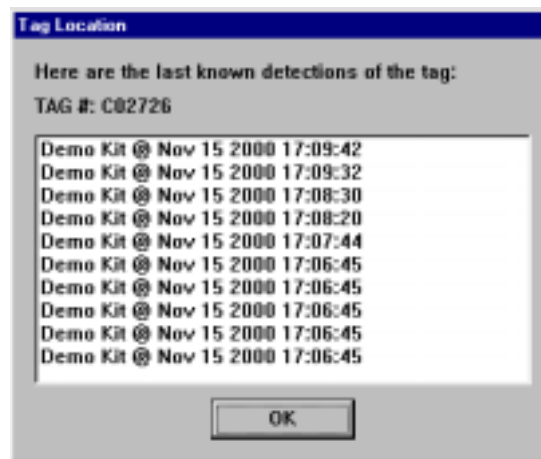
The dialog box is titled "Tag Expiry Date". It contains the text "Please enter an expiry date for the tag(s):". Below this, it shows "Expiry Date:" followed by two drop-down menus. The first menu shows "Mar" and the second shows "2002". At the bottom, there are "OK" and "Cancel" buttons.

5.8. Locate a Tag

- This feature allows you to see the last ten detections of a certain tag.
- If an infant has been abducted, this is an easy way to determine the route that the suspected kidnapper may have taken.

To locate a tag:

1. Select the tag by highlighting the appropriate line on the **Tags Management Screen**.
2. Click on 
 - A screen will appear showing the last ten detections for the selected tag.



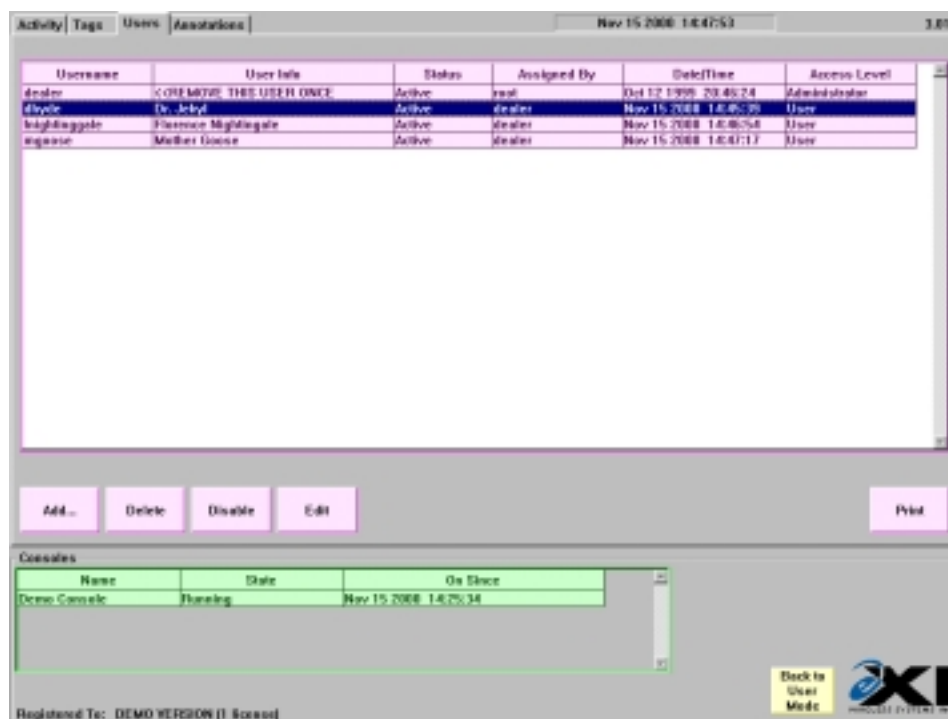
3. Click on  when you are finished viewing.

6. MANAGING SYSTEM USERS

- Only supervisors can give a user access to the system, and assign their level of access. A supervisor can assign, delete, and edit another supervisor's access level.
- Every system user requires a username and password, and these can only be assigned and entered into the system by a supervisor.
- The installer/administrator will assign access to the first supervisor. The default administrator user name is "dealer" and password is "dealer".
- After assigning access it is important that the first administrator change the default password

To access the **User Management Screen**

- Click on the **Users** tab on the Supervisor's Screen



User Management Screen - Supervisor Level

The user management screen displays:

- The current authorized users
- The usernames
- Status (Active or Disabled)
- The identity of the Supervisor assigning the user
- The last date of user file edit or entry
- The access level of the user

6.1. Adding a new user to the system

- New users can only be added from the **User Management Screen**

1. Click on



2. Enter the **Username** followed by the  key

3. Enter the **Password** followed by the  key

4. Enter the **Real Name**.

5. Select an **Access Level**

6. Choose the user's Access Level

- User** level gives access to the console to accept alarms, silence alarms, admit and discharge patients.
- Team Leader** level gives access to the **User** functions plus the **Disable Tag** feature.
- Supervisor** level gives access to all functions as described in Section 3.1.

7. Click on

The image shows two screenshots of the "Add User to System" dialog box. The top screenshot shows the empty form with fields for Username, Password, and Real Name, and radio buttons for Access Level (User, Team Leader, Supervisor). The bottom screenshot shows the form filled out with Username: jsmith, Password: jsmith, Real Name: Jane Smith, and the Supervisor radio button selected. Both screenshots have OK and Cancel buttons at the bottom.

6.2. Deleting a user from the system

- Users can only be deleted from the **User Management Screen**
 1. Select the user you wish to delete
 2. Check that you have selected the required user — this step cannot be undone.
- 3. Click on 

6.3. Disabling / Enabling a system user

- This function allows a supervisor to temporarily disable the access of a particular user; and re-enable them later.
- This may be useful when a nurse is away for a short period but is expected to return.
- Instead of deleting and re-entering all of the nurses' information, the user's data remains in the system when the user is Disabled and is quickly restored with the Enable function.
- Users can only be Disabled / Enabled from the **User Management Screen**.
 1. Select the user you wish to Disable / Enable
 2. Click on the **Disable** button or the **Enable** button as required. The user's status field will read **Disabled** or **Enabled** as appropriate

6.4. Editing a system user's access level

- A supervisor may change a user's password, "real name", and access.
- The system user name may not be changed — the user name must be Deleted and the new one Added.
- User details can only be Edited from the **User Management Screen**.
 1. Select the user you wish to edit
 2. Click on 
 3. Enter the changes

7. PRINTING LOGS

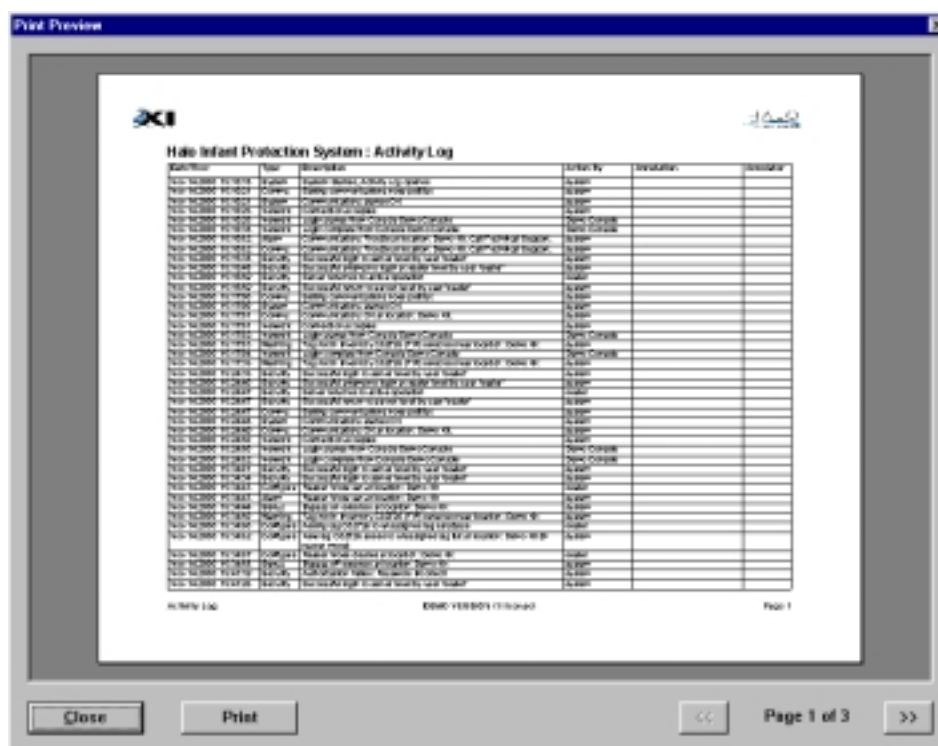
You can print the following logs:-

- activity log
- tag listing
- user listing.

To initiate printing, click on the

Print

button. A preview of the printout will appear as shown below.



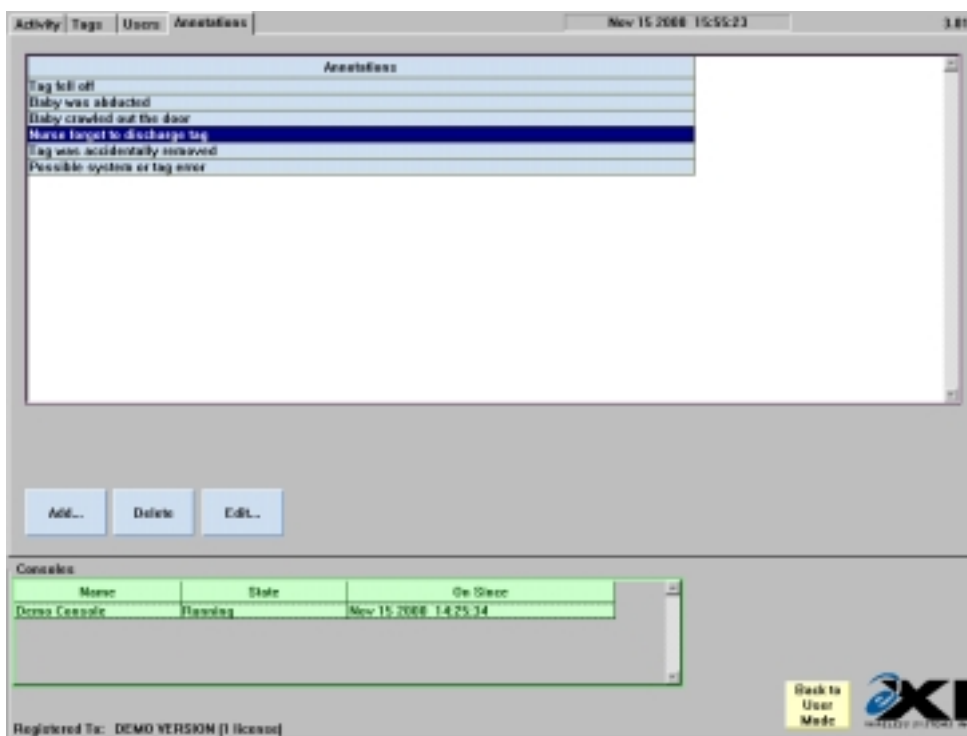
Click on **Print** to proceed with printing, or on **Close** to cancel.

8. MANAGING ALARM ANNOTATIONS

- When a user Accepts an alarm (see Section 2.4) they have the option either to enter a Note or to select a Note from a menu which a supervisor has created. The Notes are entered in the Alarm Acceptance Area of the screen.

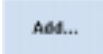


- Supervisors may add a new note, or change an existing note in the **Notes** list
- Click the **Annotations** tab on the Supervisor Screen
- You will see the list of Notes already available to users when Accepting an Alarm



Annotation Management Screen – Supervisor Level

8.1. Adding an Annotation

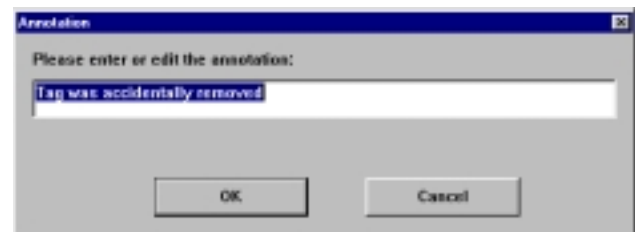
1. Click on 
2. Type in your annotation in the window that appears
3. Click  to accept changes or  to cancel .

8.2. Deleting an Annotation

1. Select the Annotation you want to delete
 2. Click on 
- The annotation will be deleted.

8.3. Editing an Annotation

1. Select the Annotation you want to change
2. Click on 
3. Edit the Annotation and select  to accept or  to undo changes.



9. SHUTTING DOWN AND RESTARTING THE SYSTEM

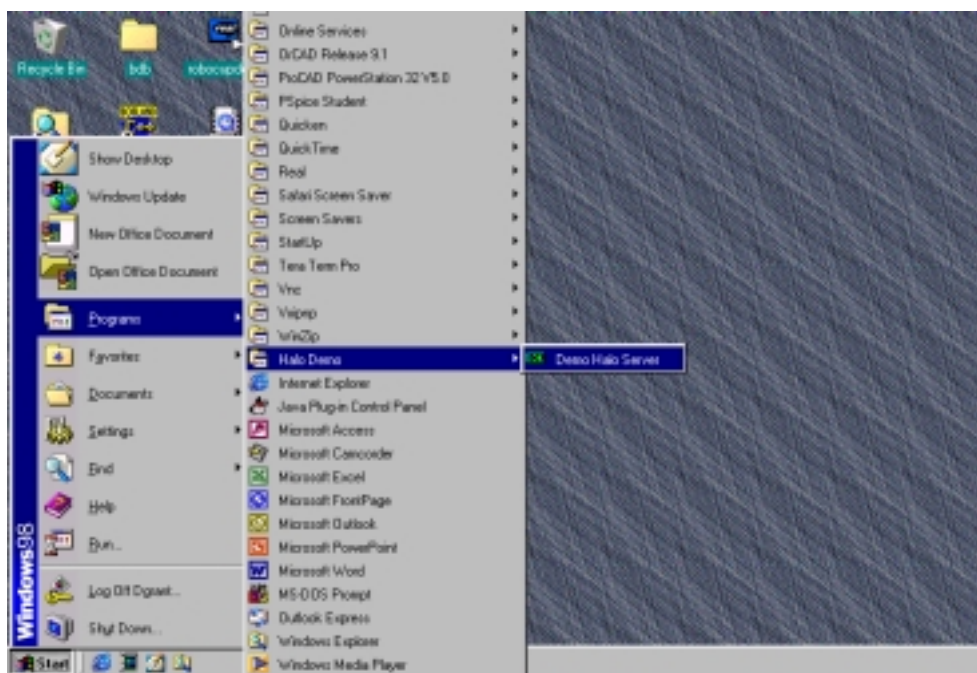
9.1. Shutting down

- The system can only be shut down from the Supervisor Level.
- We recommended that the system is shut down only for servicing because once it is shut down events will not be logged.
- Door units will remain active and the exit doors will be locked if your system is designed to do so.
- To shut down the system:
 1. Press the Ξ and Θ keys on the keyboard simultaneously.

9.2. Restarting the system — if this is required more than once a week, contact your dealer

To restart the system either

1. Turn off the computer, then turn it on again. (HALO™ will automatically launch).
2. From the Windows 98 desktop, either
 1. double-click on the “Halo Console” icon 
 - or
 2. select Start Menu, Programs, Halo, and click on 



APPENDIX A - LIMITED WARRANTY

1. **Warranty:** Subject to the limiting conditions set forth below, EXI Wireless Systems Inc. ("EXI") hereby warrants that: (a) each product, other than transponders (the "Transponders"), accompanying this warranty (the "Product"), will be free of defects in materials and workmanship for a period (the "Product Warranty Period") of two years after the date of the original sale by EXI of the Product; and (b) each Transponder accompanying this warranty will be free of defects and workmanship for a period (the "Transponder Warranty Period") of, in the case of a WTX-INF/WS Transponder, four years, and in the case of all other Transponders, three years, after the date of the original sale by EXI of the Transponder.
2. **Notification:** If the original or any subsequent purchaser (collectively, the "Purchaser") of the Product or Transponder, as the case may be, discovers a defect in materials or workmanship of a Product within the Product Warranty Period, or a Transponder within the applicable Transponder Warranty Period, the Purchaser must, within 30 days after the date of such discovery, notify EXI of such defect, and at EXI's request, return the defective Product or Transponder, as case the may be, to EXI.
3. **Repair or Replacement:** Subject to §4, upon acceptance by EXI of responsibility for the defect, EXI will, in its sole discretion, (a) in the case of a Product, either replace the Product, or provide the Purchaser with replacement parts for, or repair, the same; and (b) in the case of a Transponder, replace the Transponder at a discounted price equal to the product of: (i) the nearest whole number of months remaining in the applicable Transponder Warranty Period; and (ii) the amount of the then monthly credit available from EXI for the applicable Transponder. EXI's warranty in respect of any replacement Product, part thereof, or Transponder, as the case may be, will be for the unexpired portion of the original warranty period applicable to the relevant Product or Transponder.
4. **Exclusion:** The warranty referred to in §1 is the sole warranty made by EXI with respect to its Products and Transponders. EXI makes no other warranty or representation, express or implied, and hereby disclaims any implied warranty of merchantability or fitness for a particular purpose, statutory or otherwise, concerning its Products and Transponders. In addition, the warranty will not apply if EXI has not received a fully completed warranty registration card in respect of the Product or Transponder, as the case may be, within 30 days after the date of the original purchase from EXI of the same, or the Product or Transponder, as the case may be, or any part thereof: (a) is damaged by misuse, accident, negligence, lightning, power surge, brown-out, or leaking, damaged or inoperative batteries, or failure to maintain the Product or Transponder as specified or required by EXI; (b) is damaged by modifications, alterations or attachments thereto which are not authorized by EXI; (c) is installed, operated or repaired contrary to the instructions of EXI; (d) is opened, modified or disassembled in any way without EXI's consent; or (d) is used in combination with items, articles or materials not authorized by EXI.
5. **Limitation:** EXI will only be liable to the Purchaser for direct damages suffered by the Purchaser up to a maximum amount equal to the total amount of the purchase price actually paid by the Purchaser to EXI for the Product or Transponder, as the case may be. Specifically, EXI will not be liable for: (a) any special, indirect or consequential damage, including lost profits, lost revenues, failure to realize expected savings, or other commercial or economic losses of any kind, even if EXI has been advised of the possibility of such damage; (b) any loss or damage to any property or for any personal injury or economic loss or damage caused by the connection of the Product or Transponder, as applicable, to other devices or systems; (c) any damage or injury arising from or as a result of, misuse, abuse or incorrect installation, integration or operation of the Product or Transponder, as applicable, by persons not authorized by EXI; or (d) any defect in any batteries added to or used in conjunction with the Product or Transponder.
6. **Product Limitation:** The Purchaser (a) acknowledges that (i) the Products and the Transponders are not, nor can they be, guaranteed to prevent wandering patients, infant abductions, theft or any other event for which they were purchased, (ii) the Products and Transponders are only intended to provide additional safeguards to assist in the prevention of events such as those described in §(i), and (b) understands fully the foregoing limitations concerning the Products and Transponders, including EXI's limitation on liability described in §5, and agrees to warn, and obtain acknowledgements from, all users thereof of the same.
7. **No Additional Warranties:** The terms and conditions herein contain all the warranties and representations concerning EXI's Products and Transponders and supersede all previous negotiations, understandings, communications, representations, warranties and agreements, whether verbal or written, concerning the Products and Transponders.
8. **Deemed Acceptance:** The installation or use of the Product or Transponder by or at the direction of the Purchaser will be deemed as an acceptance by the Purchaser of the terms hereof.
9. **Governing Law:** The warranty herein will be governed by the domestic laws of the Province of British Columbia, Canada and the Purchaser hereby attorns to the exclusive jurisdiction of the laws of British Columbia. The provisions of the United Nations Convention on Contracts for the International Sale of Goods is hereby excluded.

APPENDIX B - FCC REGULATIONS

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

This equipment has been tested and found to comply with the limits for Class B Digital Device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

EXI Wireless Systems
CANADA: 287710217261A

Model No.: Patient Tag
FCC ID: HE7 PTG

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

Made in Canada

EXI Wireless Systems
CANADA: 28771031940

Model No.: Halo Infant/ECO tag
FCC ID: HE7 ETG

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

Made in Canada

EXI Wireless Systems
CANADA: 28771032080

Model No.: Halo Asset tag
FCC ID: HE7 ATG

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

Made in Canada

APPENDIX C - SYSTEM MAINTENANCE

HALO™ is designed to assist staff in providing a higher degree of safety for patients. It is not intended as the sole means of protection in preventing a wanderer or infant from leaving the premises. Regular checks to verify that your HALO™ system is operational are highly recommended.

SYSTEM MAINTENANCE SHOULD INCLUDE THE FOLLOWING STEPS:

- All Tags should be checked for physical damage after each cleaning, disinfecting or sterilization procedure.
- Each Tag should be tested for correct operation before being attached to an infant. The HALO™ software prompts for testing of Tags prior to their deployment. Please refer to the appropriate section in this manual for the instructions.
- The warranty on Tags is 2 years, and the batteries within the Tags are expected to last in excess of the warranty period, depending on the usage pattern. Do not leave Tags in the detection field for long periods of time, and store them in the foil bags supplied. Failure to do so will result in false alarms, and will reduce battery life.
- Set up a regular system check schedule to verify that the Controllers, Receivers and Tags are operational. Controllers should have the “Ready” light illuminated to show that they are powered. Check the operation of the Controller daily by starting a bypass or triggering an alarm using a Tag to ensure that it is fully operational and protecting the egress point where it is located.
- Check each Receiver on a regular basis to ensure that it can receive signals from Tags in the “Off Body” condition. Failure to regularly check for this operation may lead to failure to detect a Tag that is removed from an infant, and therefore compromising protection for the infant.
- Whenever you see a known wandering patient, look for the Tag on their person to verify they are still wearing it. This may require special knowledge as to the placement of the Tag.
- Conduct frequent back-ups of Activity Logs for future reference.