



## **User Manual**

**May 2000**

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

Revision 1.0

## Table of Contents

<b><u>P 1.</u></b>	<b><u>LIMITED WARRANTY</u></b> .....	<b>3</b>
<b><u>P 2.</u></b>	<b><u>RECORD OF CHANGES</u></b> .....	<b>4</b>
<b><u>P 3.</u></b>	<b><u>FCC REGULATIONS</u></b> .....	<b>5</b>
<b><u>P 4.</u></b>	<b><u>SYSTEM MAINTENANCE</u></b> .....	<b>6</b>
<b><u>1.</u></b>	<b><u>SYSTEM INTRODUCTION</u></b> .....	<b>9</b>
1.1.	<u>SYSTEM COMPONENTS</u> .....	9
1.2.	<u>COMPUTER DISPLAY CONVENTIONS</u> .....	9
<b><u>2.</u></b>	<b><u>USER LEVEL</u></b> .....	<b>11</b>
2.1.	<u>ENTERING AN ASSET</u> .....	11
2.2.	<u>DELETING AN ASSET</u> .....	14
2.3.	<u>SILENCING AND ACCEPTING ALARMS</u> .....	16
2.4.	<u>“STAFF SAVER” AND “LOITERING” FEATURES</u> .....	18
<b><u>3.</u></b>	<b><u>SUPERVISOR LEVEL</u></b> .....	<b>19</b>
3.1.	<u>ACCESSING SUPERVISOR LEVEL</u> .....	19
3.2.	<u>EXITING SUPERVISOR LEVEL</u> .....	20
<b><u>4.</u></b>	<b><u>ACTIVITY LOG MANAGEMENT</u></b> .....	<b>21</b>
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
<b><u>5.</u></b>	<b><u>MANAGING TAGS</u></b> .....	<b>24</b>
5.1.	<u>TAGS</u> .....	24
5.2.	<u>ADDING A NEW ASSET-TAG TO THE SYSTEM</u> .....	25
5.3.	<u>DELETING AN ASSET-TAG FROM THE SYSTEM</u> .....	26
5.4.	<u>DISABLING AN ASSET-TAG</u> .....	27
5.5.	<u>UNASSIGNING AN ASSET-TAG</u> .....	27
5.6.	<u>EDITING AN ASSET-TAG RECORD</u> .....	28
5.7.	<u>PRINTING</u> .....	28
<b><u>6.</u></b>	<b><u>MANAGING SYSTEM USERS</u></b> .....	<b>29</b>
6.1.	<u>ADDING A NEW USER TO THE SYSTEM</u> .....	30
6.2.	<u>DELETING A USER FROM THE SYSTEM</u> .....	31
6.3.	<u>DISABLING A SYSTEM USER</u> .....	31
6.4.	<u>EDITING A SYSTEM USER ACCESS</u> .....	31
<b><u>7.</u></b>	<b><u>DEALER ONLY SCREEN</u></b> .....	<b>32</b>
7.1.	<u>ACCESSING THE DEALER LEVEL</u> .....	32
7.2.	<u>DEALER ACCESS LEVELS</u> .....	32
7.3.	<u>FLOOR PLAN EDIT</u> .....	33
7.4.	<u>ADDING SYSTEM DEVICES</u> .....	34
<b><u>8.</u></b>	<b><u>SHUTTING AND RESTARTING THE SYSTEM</u></b> .....	<b>36</b>
8.1.	<u>SHUTTING DOWN</u> .....	36
8.2.	<u>RESTARTING THE SYSTEM</u> .....	36

## P 1. Limited Warranty

EXI Wireless Systems Inc. (“EXI”) hereby warrants the product(s) accompanying this limited warranty (the “Product(s)”) to be free of defects in materials and workmanship for a period of two years (excluding any batteries that may be added to or used in conjunction with the Products(s)) from the date of delivery of the original purchase of the Product(s) subject to the limiting conditions set forth below, provided that EXI has received notification of such defects no later than 30 days after expiration of the applicable warranty period and provided further that EXI has received a fully completed registration card (below) within 30 days from the date of original purchase of the Product(s).

The responsibility of EXI under this warranty is and shall be limited to repairing or replacing the Product(s) or any part thereof determined by EXI in its sole discretion to be defective in workmanship or material.

The installation of the Product(s) shall be deemed as acceptance by the original purchaser and any subsequent purchaser of the Product(s) (collectively the “Purchaser”) of the terms set out in this limited warranty including the following further limiting conditions:

- (a) EXI shall not be responsible for any repair or replacement of any Product(s) which has been found, upon inspection, to have been subjected to abuse, misuse or negligence, or any damage attributable to accident, lightning, power surge, brown-out, leaking, damaged or inoperative batteries or to have been installed, altered or repaired contrary to factory designated procedures without the prior written consent of EXI;
- (b) It is understood, and the Purchaser agrees further to so inform any user of the Product(s) that the Product(s) is not, nor can it be, infallible in the detection of wandering patients, the prevention of infant abduction, the prevention of theft of assets or any other contemplated use of the Product(s). **The Purchaser will warn all users and acknowledges on it’s own behalf that it has read and understands the above-mentioned limitations of the Product(s).** The Purchaser further acknowledges that the Product(s) are solely intended to provide an additional safeguard in notifying staff and accordingly do not guarantee the prevention of wandering patients or the attempted abduction of an infant or the theft of assets;
- (c) It is further agreed by the Purchaser that the Purchaser has received no additional promises or statements of fact from EXI or its agents relative to the Product(s) upon which the Purchaser might have relied in purchasing the Product(s);
- (d) The warranty set out above excludes and is in lieu of all other express or implied warranties, conditions or obligations, and no person is authorized to give any further representation or warranty or assume any further obligation on behalf of EXI. Although the Purchaser may have other rights, as they may vary from State to State or Province to Province, where it is legally possible to do so any statutory warranty is hereby expressly excluded. The warranty is subject to the domestic laws of Canada and the Purchaser agrees to attorn to the jurisdiction of the courts of competent jurisdiction in the Province.
- (e) EXI shall not be liable for any damages, whether direct or, indirect, incidental, consequential or arising out of contract or tort with the sole exception of the warranty set out above and any rights expressly created by applicable statute.

THIS WARRANTY IS VALID ONLY IN THE USA AND CANADA

## **P 2. Record of Changes**

May 2000      Revision 1.0      Initial Release

### P 3. 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: TBD	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: TBD	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 re-	

ceived, including interference that may cause undesired operation.  
Made in Canada

## P 4. System Maintenance

ASSETRAC is designed to assist staff in providing a higher degree of safety for their equipment . **It is not intended as the sole means of protection in preventing an item from leaving the premises.** Regular checks to verify that your ASSETRAC system is operational is 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 ASSETRAC software prompts for testing of Tags prior to their deployment. Please refer to the appropriate section in this manual for the instructions.

The warrantee on Tags is 3 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 "Tag Removal" 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.

## **Intended Audience**

This manual is intended for system users (typically duty nurses) 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 Assetrac system features a very simple user interface that steps the user through and provides instructions at each step.

## About Assestrac Protection System

Assestrac is a premium asset protection system. Assestrac works in conjunction with the EXI Asset tag transponder that is capable of sensing if it has been removed from a piece of equipment. Assestrac is an electronic system, which, in conjunction with staff diligence, creates a secure perimeter to deter asset theft .

Assestrac will detect if an asset is near a controlled exit and invoke countermeasures. The system will identify the asset, 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 Assestrac system has three separate access levels:

- User
- Supervisor
- Dealer

Level	Password required	Functions	Access Management
User	Yes	Enter Asset Delete Asset Accept/Silence alarms Toggle between floor plans (No Password required)	Access controlled by Supervisor or Dealer level users
Supervisor	Yes	All user functions Manage user list Assign usernames and passwords View and annotate activity logs Add/Delete tags from fleet Initiate System Data Backups Print logs Exit the Assestrac system	The first Supervisor is setup by the installing dealer. This Supervisor may add more assigned supervisory access.
Dealer	Yes	All user/Supervisor functions System Diagnostics System modifications Importing floor plans	Controlled by EXI

## 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 should have a unique name.

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

## System Support

For system service or support contact your installing dealer. Your dealer is:

Name: \_\_\_\_\_

Phone: \_\_\_\_\_

Or contact:

EXI Wireless Systems  
100-13551 Commerce Parkway  
Richmond, BC  
Canada V6V 2L1  
Ph: 1-800-667-9689  
Fax: 604-207-7760  
Web: [www.exi.com](http://www.exi.com)



## 1. System Introduction

### 1.1. System Components

**ASSETRAC Software:** Primary user interface that assist in the assignment and tracking of Transponders, and displays alarms and other activities in graphical format. 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, allow keypad input for door bypass, and offer a “Staff Saver” and “Loiter” feature. The “Staff 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 Removal” condition in its area, as does a Receiver.

**Receivers:** Detects “Tag Removal” condition when a Tag is removed from an asset, and reports this activity to the computer.

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

#### Tag-initiated-Communications (TIC)

This alarm is initiated in the event that a Tag is removed from a piece of equipment. This occurs due to the fact that the Tag tamper switch is no longer attached to an asset.

#### Tag-in-field Communications (TIF)

This alarm is initiated when a Tag enters an area protected by a Controller. The Controller emits a constant field of radio waves which 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 RF field.

### 1.2. Computer Display Conventions

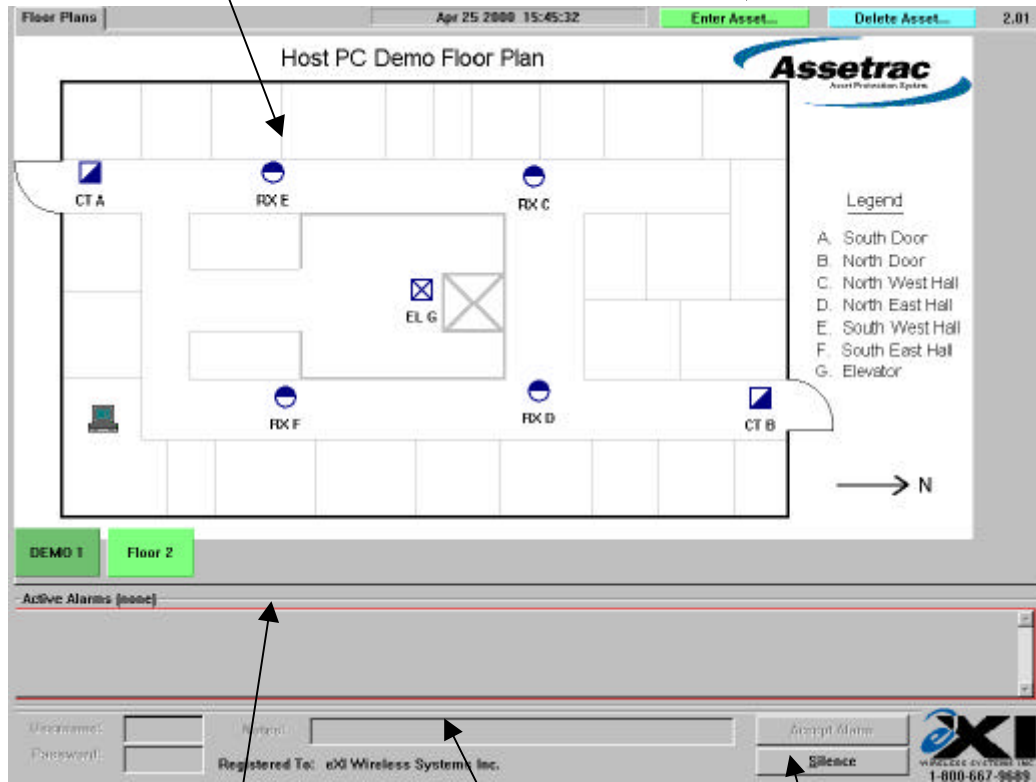
The computer displays various types of information, which is color coded to differentiate between the Dealer, Supervisor and User modes. In addition, the “Icons” that display the locations of the various system components such as the Controllers and the Receivers, and the on-screen “buttons” may also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

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

Floor Plan area.

- Controllers shown as half-filled square icons
- Receivers shown as half-filled circular icons
- Elevators shown as square icon with "X"
- Blue: Normal, Yellow: Pre-Alarm condition, Flashing Red: Full Alarm condition
- Arrow points at device(s) corresponding to selected alarm in Active Alarm field

Asset **Enter** and **Delete** buttons



Floor Plan Buttons

- Green: Normal
- Blue: Indicates that the cursor is positioned over button
- Yellow: Indicated Pre-alarm condition on floor
- Red: Alarm condition on this floor

Active alarms field

- Red: Normal alarm color
- Blue: Selected alarm

Alarm Silence and Accept field.

Normally grayed characters.


“Silence” button is active upon selecting an alarm from the Active Alarm field.

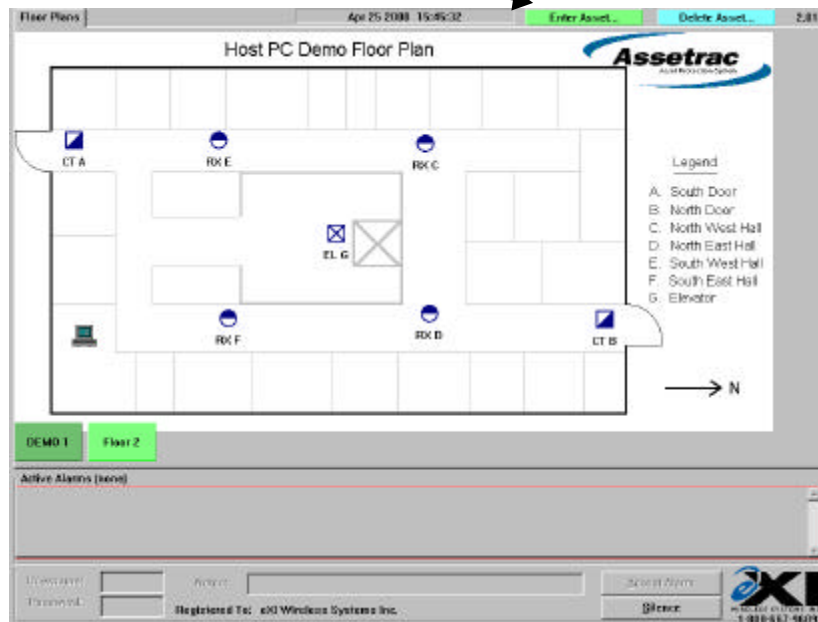
“Accept Alarm” button is active after valid Username and Password are entered.

## 2. User Level

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

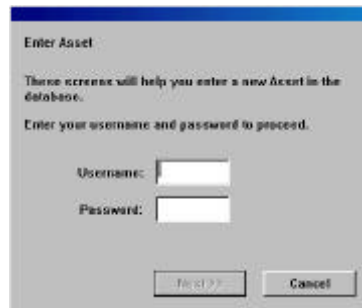
### 2.1. Entering an Asset


1. Select the  button on the top right of the screen.



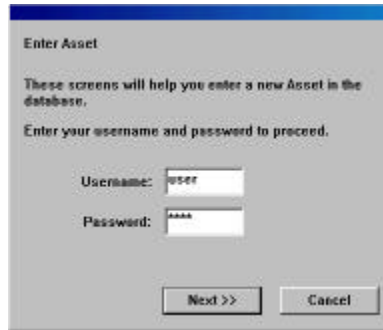
Main Screen - User Level

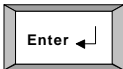
2. The system will ask for your **Username** and **Password**. Type in your **Username** as assigned by your supervisor.



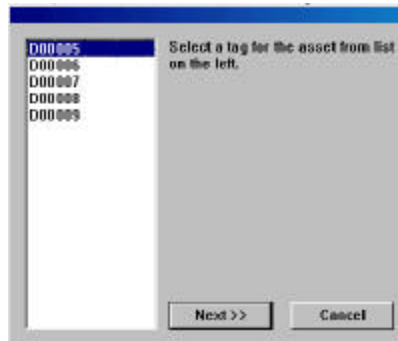
3. Press the  key on the keyboard

4. Type in your **Password**



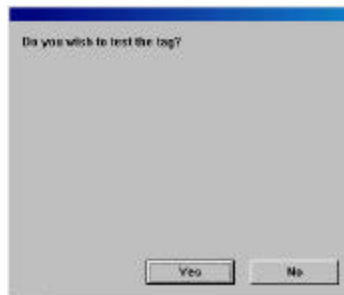
5. Press  key on the keyboard, or click on the **Next** button

6. The system will now ask you to choose a tag. Select the **Tag Serial Number** corresponding to the tag you wish to use.



*Note: Each asset tag has a unique serial number on the side of the tag. The system will list all of the available tags registered in the system but not yet assigned to an asset.*

7. The system will ask if you wish to test the tag. Select **Yes** if you wish to do so. The system will navigate you through the process.

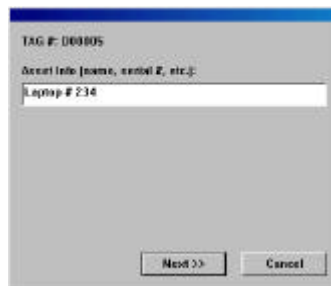


**Note:** During this test, the system is verifying the tag serial number, testing the tag removal alarm and generating an activity log entry to document the test.

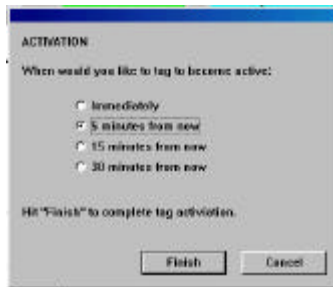
**Hint:** Ensure the bottom of the tag is held stable on a flat surface during the test for about 10 seconds prior to removing. If the test fails, try it once more on your wrist.

Once the tag is verified, the system will automatically take you to the next step in the admit process.

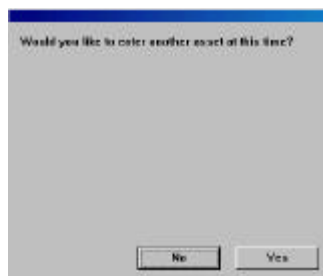
- 8. Enter the **Asset Name** in any format you wish. Click 



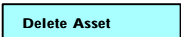
- 9. Choose when you would like the tag removal alarm to be activated by selecting the appropriate **Activation delay box**. Select **Finish**. Delays apply to sensing “tag removal” or TIC alarms only. Tag will still initiate alarms and control at egress points

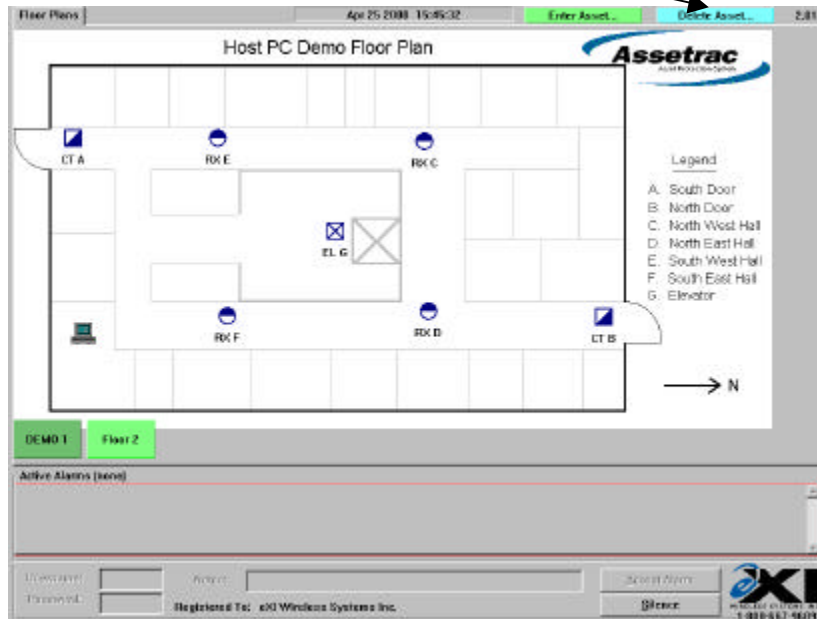


- 10. You have now admitted the infant. If you wish to admit another, select **Yes**. If not, select **No**.

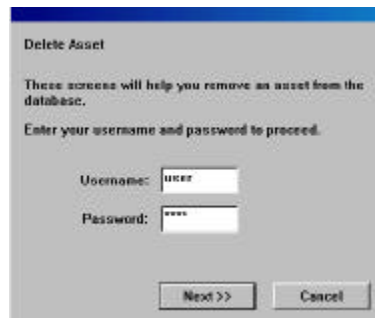


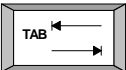
### 2.2. Deleting an Asset

1. Select  the button on the top right of the screen.

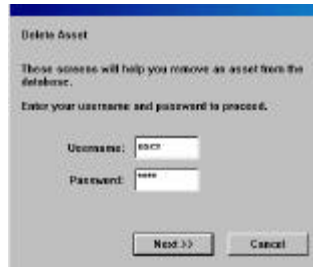



2. The system will ask for your **Username** and **Password**. Type in your username as assigned by your supervisor.



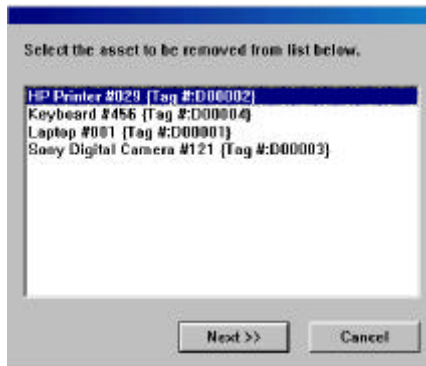
3. Press the  key on the keyboard

- 4. Type in your **Password**

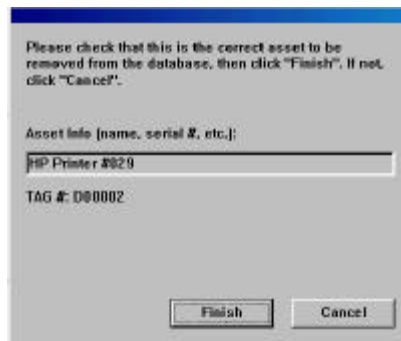


- 5. Press the  key on the keyboard, or click on the **Next** button.

- 6. Select the **Asset** you wish to delete. Select **Next**.



- 7. The system will redisplay the **Asset Name** for you to verify. Select **Finish** if this is the correct infant. If it is not the infant you wish to discharge, select **Cancel** and start from step 1 again.



*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. Silencing and Accepting Alarms

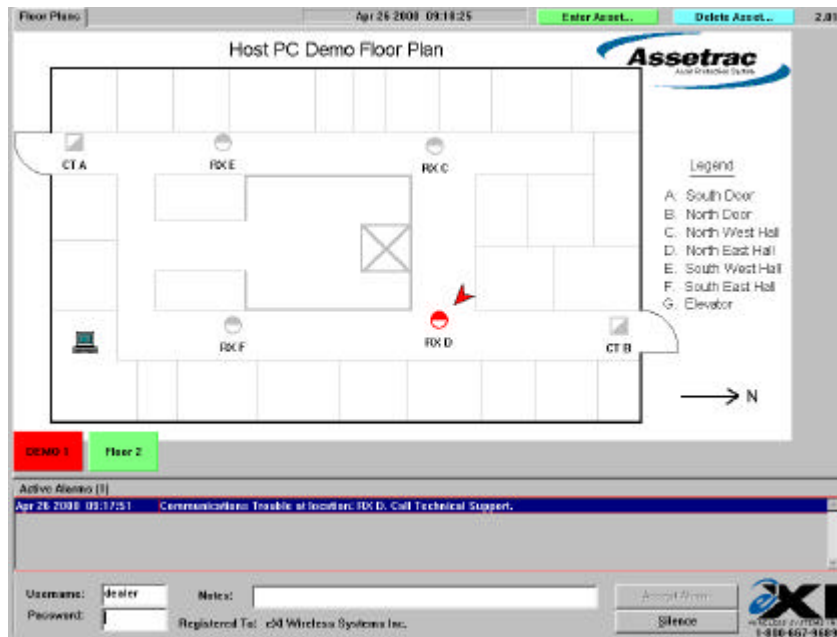
The Assestrac system will alarm when:

- An assigned asset tag has been removed from an asset (tag removal or TIC)
- When an asset tag is detected near a controlled egress area (In field or TIF)

When an alarm occurs, the system will:

- Identify the asset 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.

#### Main Screen - User Level

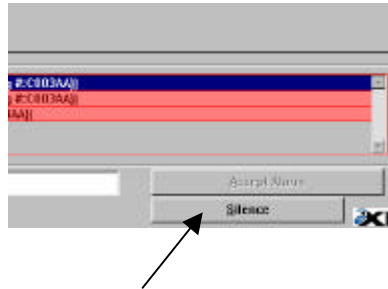


Alarm Acceptance Area

During an alarm, the alarm acceptance area becomes active.



### Silencing an alarm



To silence the audible alarm, select **Silence** in the alarm acceptance area.

Note: You must accept the alarm to clear the alarm condition. Silencing simply silences the audible alarm while the incident is investigated.

### Accepting an alarm

To accept an alarm, select the alarm condition in the active alarms field. If only one alarm exists, it will automatically be selected.

A screenshot of the alarm acceptance interface. At the top, there are four colored buttons: 'Lower Floor West' (green), 'Lower Floor East' (red), 'Upper Floor West' (green), and 'Upper Floor East' (green). Below these is a table of 'Active Alarms' with columns for time and description. Underneath the table are input fields for 'Username:', 'Password:', and 'Notes:'. An 'Accept Alarm' button is at the bottom. Six numbered steps with arrows and keyboard icons describe the process: 1. Type in your Username (arrow to Username field); 2. Press TAB (arrow to Password field); 3. Type in your Password (arrow to Password field); 4. Press TAB (arrow to Notes field); 5. Enter a note in the Notes field (optional); 6. Select (arrow to Accept Alarm button).

1. Type in your **Username**
2. Press
3. Type in your **Password**
4. Press
5. Enter a note in the **Notes** field (optional)
6. Select

The system will log the following incident details:

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

The Assetrac system is usually set up to create multiple detections of an alarm for security purposes. When multiple system devices see the same tag in alarm, the system will condense this into one incident for the staff member to accept.

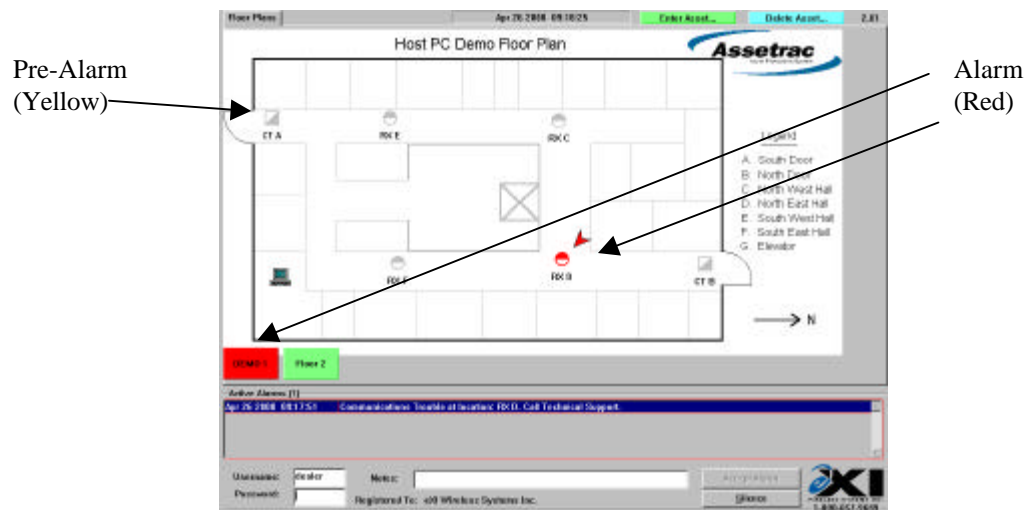
When multiple alarms occur, the staff member must accept each alarm before the system will clear the alarms. This normally means more than one infant tag alarmed simultaneously.

All alarms are maintained in a log for supervisor review.

#### 2.4. “Staff Saver” and “Loitering” Features

If the system is installed with the “Staff Saver” feature, Tags detected at egress points which are secured will not set off nuisance alarms. A Tag detected near a door that is closed will result in the 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. An alarm is initiated if the door was to be opened while the Tag was still present at the door. For this feature, the door has to be equipped with a magnetic switch to sense whether it is in the closed or open position.

If the tag remains at the door for a period of one minute or more, an egress alarm will be initiated and the button on the screen and the icon will turn to red. This is the “Loitering” feature.

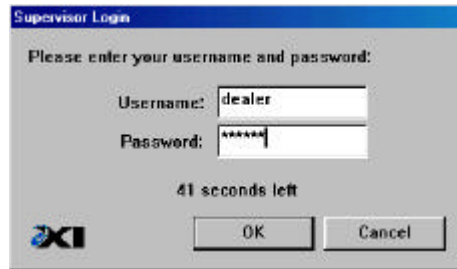


### 3. Supervisor Level

#### 3.1. Accessing Supervisor Level

1. Press the  and  keys on the keyboard simultaneously.

2. The system will ask for your **Username** and **Password**.



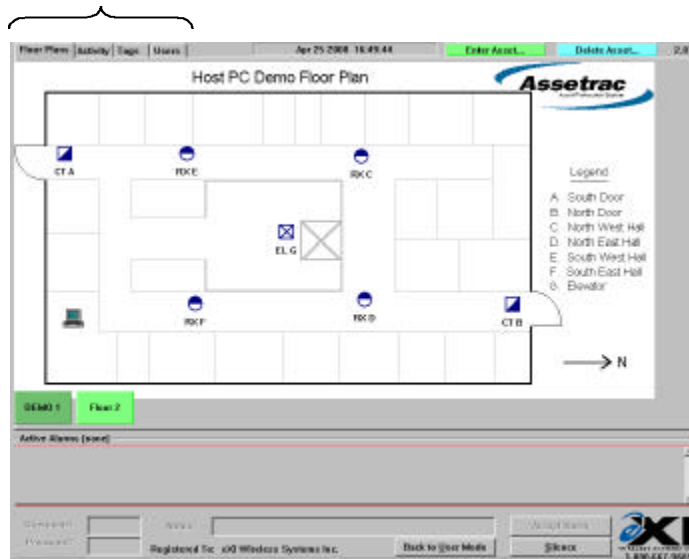
3. Enter you **Username**

4. Press the  key on the keyboard

5. Enter your **Password**

6. Select **OK**. The Supervisor screen will appear as shown below.

Supervisor Tabs



Once in Supervisor mode, three Supervisor function tabs appear:

- Activity
- Tags
- Users

#### Supervisor Level Functions

<b>Supervisor tab</b>	<b>Access</b>	<b>Functions</b>
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 Asset information for tag View current asset population
Users	Supervisor only	Add or delete a user Disable or Activate a user Change user passwords

### 3.2. *Exiting Supervisor Level*

To exit the Supervisor level, select the

**Back to User Mode**

button at the bottom of the screen.

## 4. Activity Log Management

### 4.1. Activity Logs

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

- Asset 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

To enter the activity log area, you must first be in the Supervisor access area (See section 3.1). To view the activity log, select **Activity Log** from the Supervisor function tabs.

#### Activity Screen - Supervisor Level

Date/Time	Type	Description	Action By	Annotate
Apr 25 2000 16:15:18	System	System Started, Activity Log opened	system	
Apr 25 2000 15:55:07	System	System Shutdown, Activity Log closed	system	
Apr 25 2000 15:55:07	System	Communications stopped OK	system	
Apr 25 2000 15:55:07	System	Shutdown of Asset Protection System by user 'dealer'	dealer	
Apr 25 2000 15:54:26	Configure	Asset Registered: Keyboard #456 (Tag #:D00004), active immediately	dealer	
Apr 25 2000 15:53:08	Configure	Asset Registered: Sony Digital Camera #121 (Tag #:D00003), active	dealer	
Apr 25 2000 15:52:32	Configure	Asset Registered: HP Printer #029 (Tag #:D00002), active immediately	dealer	
Apr 25 2000 15:51:44	Configure	Asset Registered: Laptop #001 (Tag #:D00001), active immediately	dealer	
Apr 25 2000 15:51:08	Configure	Adding tag D00009 to unassigned tag database	dealer	
Apr 25 2000 15:51:08	Configure	Adding tag D00008 to unassigned tag database	dealer	
Apr 25 2000 15:50:49	Configure	Adding tag D00007 to unassigned tag database	dealer	
Apr 25 2000 15:50:39	Configure	Adding tag D00006 to unassigned tag database	dealer	
Apr 25 2000 15:50:32	Configure	Adding tag D00005 to unassigned tag database	dealer	
Apr 25 2000 15:50:22	Configure	Adding tag D00004 to unassigned tag database	dealer	
Apr 25 2000 15:50:13	Configure	Adding tag D00003 to unassigned tag database	dealer	
Apr 25 2000 15:50:07	Configure	Adding tag D00002 to unassigned tag database	dealer	
Apr 25 2000 15:49:57	Configure	Adding tag D00001 to unassigned tag database	dealer	
Apr 25 2000 15:49:31	Security	Successful attempt to login at dealer level by user 'dealer'	system	
Apr 25 2000 15:47:50	System	Communications started OK	system	
Apr 25 2000 15:47:50	Comms	Setting communications node poll list	system	
Apr 25 2000 15:47:50	System	System Started, Activity Log opened	system	
Apr 25 2000 15:46:17	System	System Shutdown, Activity Log closed	system	
Apr 25 2000 15:46:17	System	Communications stopped OK	system	

Active Alanna (none)

Obnoxious:  Notice:  Accept Alarm

Registered Tel: EXI Wireless Systems Inc. Back to User Mode Silence

EXI WIRELESS SYSTEMS INC. 1-800-567-9689

The system will show the system activity log. Each screen will display one page of alarm activity.

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 find a particular activity event, first navigate to the day of interest by selecting the “Day” buttons.

To step one day back, select



To step one day forward, select



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

#### **4.3. Adding a Supervisor annotation to an alarm**

To add a Supervisor annotation, select the particular alarm you wish to annotate by highlighting it. You may highlight the alarm by navigating the mouse pointer anywhere on the alarm line and clicking the left mouse button on the activity of interest.

1. Select



2. Enter the note

3. Select **OK**

#### 4.4. Backing up Activity Logs

The system is capable of storing 14,000 events in the Activity Logs. Remember that all system activities, including alarm conditions, pre-alarm conditions, door access and bypass activity are logged.

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.

Activity Logs may be backed up on the computer Hard Drive while in Supervisor mode. To initiate a back-up, simultaneously press the



and



keys on the Keyboard.

The back-up log file is stored under the "Assetrac" directory on the Hard Drive of the computer. The file is date stamped to identify the different back-up files. If it is desired to make copies of these files for archiving, you will need to exit the ASSETRAC 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 asset to have an Asset 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 asset information for an assigned tag.
- Print the list of tags in the fleet.

To manage tags, you must be in the Supervisor level of the system.

Select the **Tags** button on the top left of the screen.



**Tag Management Screen - Supervisor Level**



Tag #	Asset Info	Status	Assigned By	Date/Time
D00001	Laptop #001	Active	dealer	Apr 25 2000 15:51:44
D00002	HP Printer #029	Active	dealer	Apr 25 2000 15:52:32
D00003	Sony Digital Camera #121	Active	dealer	Apr 25 2000 15:53:08
D00004	Keyboard #456	Active	dealer	Apr 25 2000 15:54:26
D00005		Unassigned		
D00006		Unassigned		
D00007		Unassigned		
D00008		Unassigned		
D00009		Unassigned		

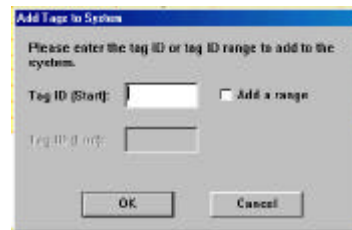


**5.2. Adding a new Asset-Tag to the system**


To add a new Asset-Tag to the system, you must first navigate to the **Tags** screen in Supervisor level area. You may add Asset-Tag’s manually or by using the Assestrac network to read them.

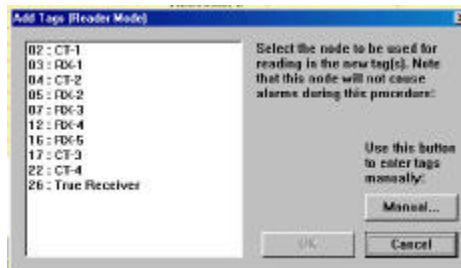
To add manually:

1. Select 
2. Select 
3. Enter in the serial number of the new tag
4. Select **OK**



To use the system to read the tags in:

1. Select 
2. Select the nearest device in the system from the list shown on the left of the “**Add Tags**” panel. After selecting the device and clicking on “OK”, a “Reader Mode” alarm for the device will appear in the Active Alarm Field. This indicates that the device selected has entered Reader Mode and is not available for normal alarms, and is therefore in bypass state.



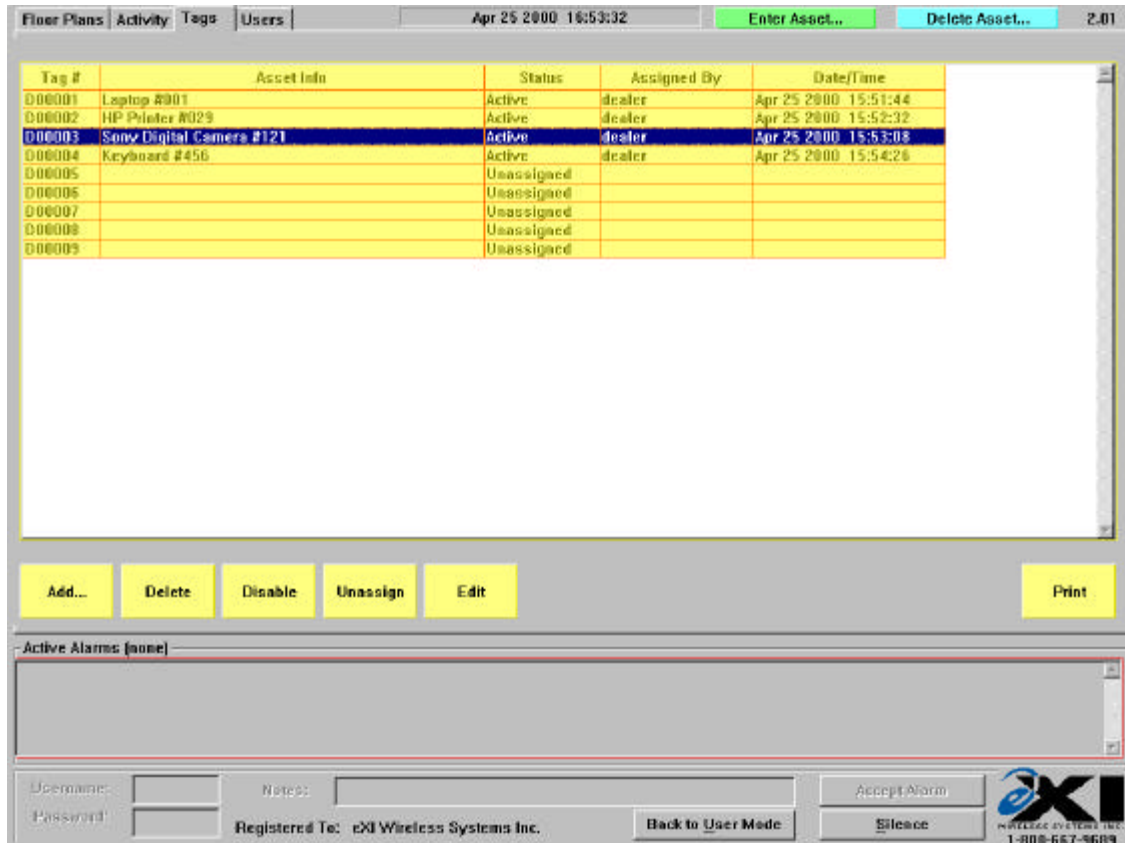
3. Wave the tag in the air ensuring you are not contacting the bottom of the tag. The tag should read in automatically.
4. Clear the “Reader Mode” alarm to ensure that the device comes back on line and is ready to report alarms.

**Note:** The automatic reader mode uses the Controller or Receiver closest to the computer that you are working on to enable the reading of the Tag serial number. Ensure you clear “Reader Mode” alarm to re-enable this device.

### 5.3. Deleting an Asset-Tag from the system

To delete an Asset-Tag, you must first navigate to the **Tags** screen in Supervisor level.

#### Tags Screen - Supervisor Level



To delete a tag:

1. Select the tag you wish to delete by navigating the mouse pointer anywhere on the line corresponding to the tag on the screen.

Note: The line will change color when you have selected it (See example above)

2. Select

Delete

#### 5.4. Disabling an Asset-Tag

To disable an Asset-Tag, you must first navigate to the **Tags** screen in Supervisor level.

Note: You may only disable tags that are currently assigned to an infant.

To temporarily disable the Asset-Tag in the system:

1. Select the tag to be disabled by navigating the mouse pointer anywhere on the line corresponding to the tag on the screen.

2. Select

**Disable**

Note: The tag disabling allows for removal of the tag from the asset without an alarm. The asset is not actually discharged from the system. Once you have disabled the tag you are responsible to enable it again or remove the infant from the system in user mode or supervisor mode. This event is captured in the Activity log.

#### 5.5. Unassigning an Asset-Tag

As a supervisor, you may unassign an Asset-Tag. To unassign an Asset-Tag, you must first navigate to the **Tags** screen in Supervisor level.

Note: Once a tag is unassigned, the asset name will be removed from the system.

To unassign a tag:

1. Select the tag to be unassigned by navigating the mouse pointer anywhere on the line corresponding to the tag on the screen.

2. Select

**Unassign**

The tag will automatically be unassigned.

### 5.6. Editing an Asset-Tag Record

An Asset-Tag record may be edited if the tag is assigned to an asset. The edit function allows a Supervisor to edit the name associated with the tag serial number. To edit an Asset-Tag record you must be in the Tags area in the Supervisor level. To edit an Asset-Tag parameter listing:

1. Select the tag to be edited by navigating the mouse pointer anywhere on the line corresponding to the tag on the screen.


2. Select



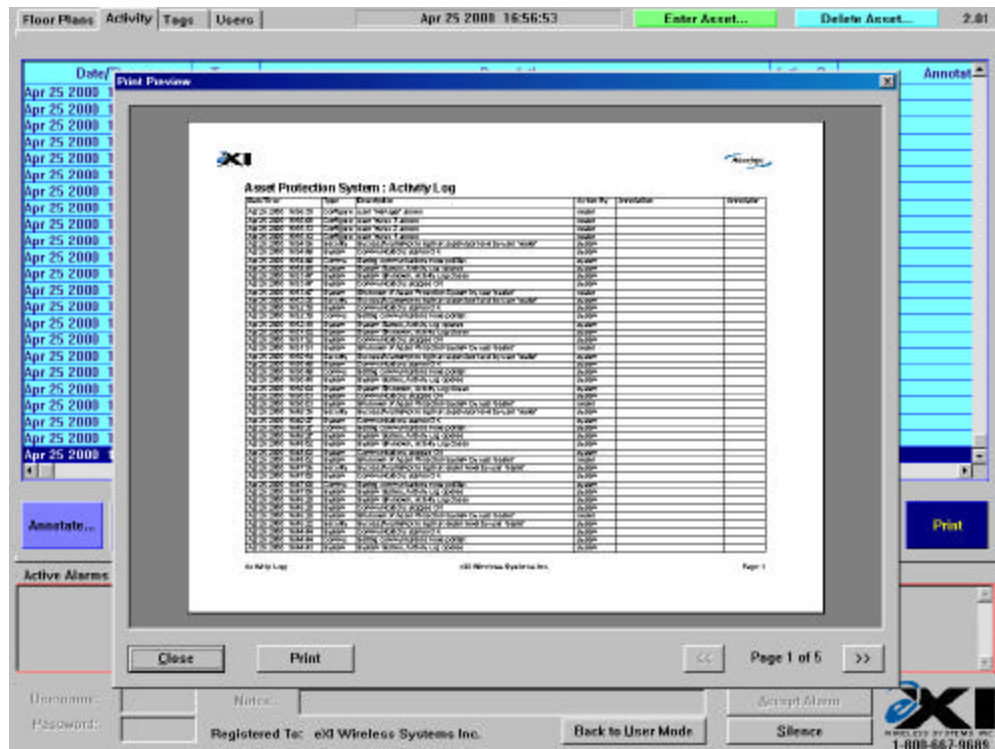
The system will now display the name currently assigned to the tag. You may edit the name by selecting the name and typing in the edits.

### 5.7. Printing

Hard copy printing is supported for all the primary logs. It is necessary for a printer to be connected to the Assestrac computer to be able to print hard copies of the logs.

To initiate printing, click on the  button. A preview of the print-out will appear as shown below.

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



## 6. Managing System Users

As a supervisor, you control who has access to the system. Every activity in the system requires a user-name and password that is assigned and entered into the system by a supervisor.

To manage users, you must have accessed the Supervisor level of the system (See section 4.1)

Select **Users** in the top left-hand corner of the screen using the mouse.

### User Management Screen - Supervisor Level

Username	User Info	Status	Assigned By	Date/Time	Access Level
dealer	<<DEALER TO REMOVE THIS USER	Active	root	Mar 25 1999 12:56:29	Dealer
manager	Kim	Active	dealer	Apr 25 2000 16:56:38	Supervisor
nurse 1		Active	dealer	Apr 25 2000 16:55:12	User
nurse 2	Mary	Active	dealer	Apr 25 2000 16:55:33	Supervisor
nurse 3	Jane	Active	dealer	Apr 25 2000 16:56:08	User

Active Alarms [none]

Username:  Password:  Notes:

Registered To: EXI Wireless Systems Inc. Back to User Mode Accept Alarm Silence

EXI WIRELESS SYSTEMS INC. 1-800-667-9609

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

To add a new user, you must first navigate to the **Users** screen in Supervisor level.

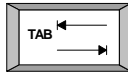
1. Select



2. The system will then ask you to enter in a username, password and real name.

3. Enter in the username you wish to assign to the user, followed by the

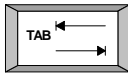
4. Press the



key on the keyboard

5. Enter in the password assigned to the new user

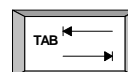
6. Press the



key on the keyboard.

7. Enter in the common name for the user (usually their full name)

8. Press the



key on the keyboard.

9. If the user is to have Supervisor level access select **Supervisor**

10. Select **OK**

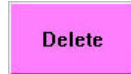
Note: It is suggested that supervisor access be carefully controlled. Any supervisor may assign, delete or edit another supervisors access level.

## 6.2. Deleting a user from the system

To delete a user from the system, you must first navigate to the user area in the Supervisor level.

1. Select the user you wish to delete by clicking anywhere on the line corresponding to the user on the screen

2. Select



**Caution!:** Ensure you have selected the correct user prior to selecting delete. This step cannot be undone.

## 6.3. Disabling a system user

The user disable function allows a user to temporarily disable the user access of a particular user. This may be useful when a nurse is on leave of absence but is expected to return. Instead of deleting and re-entering all of the nurses' information, a Supervisor may leave the user in the system but disable access.

To disable a user, you must first navigate to the user area in the Supervisor level.

1. Select the user you wish to disable by clicking anywhere on the line corresponding to the user on the screen.

2. Select



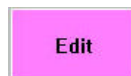
The user status field should now read "disabled" for that user.

## 6.4. Editing a system user access

A Supervisor may change a user's password or name associated with the system username. This may be useful for surname changes etc. To edit a user file, you must first navigate to the Supervisor level and user area.

1. Select the user you wish to edit



2. Select

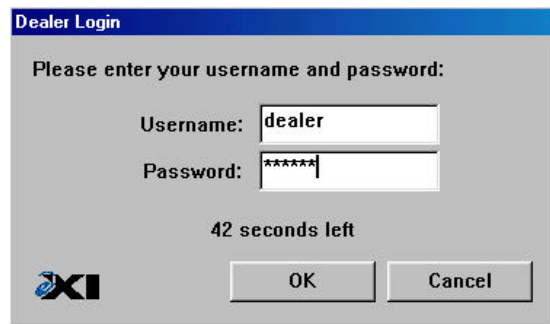


**Note:** You may change a users password and "real" name. The system username is fixed. If you wish to change the username, you will have to delete and then add the user into the system again.

## 7. Dealer Only Screen

### 7.1. Accessing the Dealer Level

1. Press the   keys on the keyboard simultaneously.
2. Enter your **Username** and **Password** and click **OK**.



### 7.2. Dealer Access Levels

The Dealer has access to all levels of the Assetrac system and is mainly responsible for:

Level	Password required	Functions	Access Management
Dealer	Yes	<ul style="list-style-type: none"> <li>• System Configurations</li> <li>• Floor Plan Editor</li> <li>• Assign usernames and passwords</li> <li>• View and annotate activity logs</li> <li>• Add/Delete tags from fleet</li> <li>• Initiate System Data Backups</li> <li>• Exit the Halo system</li> </ul>	EXI & Dealers





#### **7.4. Adding System Devices**

The final screen is the “Dealer Only” screen, which is unique to the Dealer mode. This screen contains a list of all devices present on the Assetrac network, and allows the addition and deletion of devices as well as the setting up of the communications parameters of the network. The communications port default value of “COM2”, and the baud rate of “57600” bits per second should never need to change, and are there only for future considerations.

Floor plans can be re-arranged in any order by clicking the “**Re-order**” button.

**Filter Door Events** is defaulted “ON”, this means the system will ignore all door open and closure activities and will not display in the activity log. (*Recommended*)

**TIC Notice & TIF Notice** Alarms are defaulted “ON”

Floor Plans | Activity | Tags | Users | Dealer Only | Apr 25 2000 17:06:27 | Enter Asset... | Delete Asset... | 2.01

**Nodes**

Node ID	Node Name	Type	Node Number
03	CF A	Controller	012345
04	CF B	Controller	123456
05	RX C	Receiver	234567
06	RX D	Receiver	345678
07	RX E	Receiver	123457
08	RX F	Receiver	123458
09	EL G	Elevator	123459

**Add Node to System**

Please enter the details of the node you would like to add to the system:

Node ID:  Node Number:

Node Name:

Controller  Elevator  Receiver

**Communications**

Port:

Baudrate:

**TIC/TIF Alarm**

TIC Notice  TIF Notice

Port:

Baudrate:

**Floor Plans**


**Filters**

Filter Door Events

**Active Alarms [none]**

Username:  Password:  Notes:

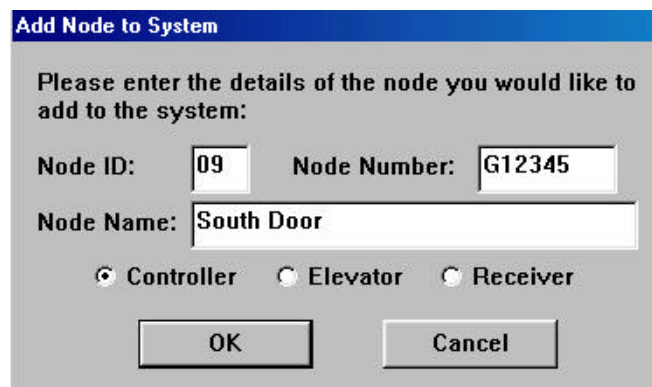
Registered To: eXI Wireless Systems Inc.



1-800-667-9689

New System Devices such as Controllers, Receivers and Elevator Controllers can be added to the system if necessary. Remember that all devices in the original installation plan are already added into the application at the factory, and therefore there should be very little need to add more in the field. This may only become necessary because of substituting a RIM device, or adding more nodes. (*Refer to Install Manual*)

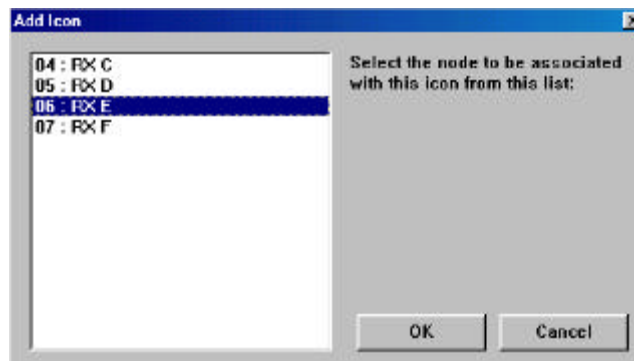
In order to add devices, click on the “Dealer Only” tab and click on “Add”. Fill in the appropriate information in the “Add Node to System” panel and click on “OK”. Note that the “Node Number” is the serial number of the RIM associated with the device added.



The screenshot shows a dialog box titled "Add Node to System". It contains the following fields and controls:

- Text: "Please enter the details of the node you would like to add to the system:"
- Node ID: 09
- Node Number: G12345
- Node Name: South Door
- Radio buttons:  Controller,  Elevator,  Receiver
- Buttons: OK, Cancel

The node that was just entered will need to be placed on the appropriate floor and at the physical location of the device that the icon represents. Select the appropriate icon from the Dealer Toolbar and drag it to the correct location on the floor plan. An “Add Icon” panel will show you the list of nodes available for placement. Highlight the appropriate node and click “OK” to complete the placement.





The screenshot shows a dialog box titled "Add Icon". It contains the following elements:

- List of nodes: 04 : RX C, 05 : RX D, 06 : RX E (highlighted), 07 : RX F
- Text: "Select the node to be associated with this icon from this list:"
- Buttons: OK, Cancel



## 8. Shutting and Restarting the System

### 8.1. Shutting down

If you wish to shut down the system, you must first enter the Supervisor level (See Section 2.1). Once in Supervisor level, Press the  and  keys twice on the keyboard simultaneously. Enter user name

and password to shut down.

**Caution!:** Once you have exited the software, the system will no longer log events. The door units will remain active and lock the exit doors if your system is designed to do so. It is recommended that the system is shut down only for servicing.

### 8.2. Restarting the system

To restart the system, you may:

1. Cycle the power on the computer. (Assetrac will automatically launch)
2. While in the Windows 98 operating system, double click on the “Assetrac Console” icon on the desktop, or you can select **Start – Programs – Assetrac**, and click on Asset Protection System.



**Note:** If your system requires restarting more than once a week, contact your dealer and have them investigate the problem.