EquipCommand® Enterprise Software: ImpactManager® RF

Version 3.6.0

500 Water Street
Newport, DE 19804
T: 302.514.0600
F: 302.636.0100
www.totaltraxinc.com

Technical Support

TotalTrax, Inc. technical and customer support is provided free of charge at the following telephone numbers.

Technical Service	T: (855)-895-7721 F: (940)-549-0674
Customer Service	T: (855)-895-7720 F: (940)-549-0651

Technical support business hours are 7:00 a.m. to 5:00 p.m. CST, Monday - Friday.

Copyright 2012 TotalTrax, Inc.

This document is written and published by TotalTrax, Inc. All rights reserved. TotalTrax, Inc. reserves the right to make changes in this document and to its products and pricing without notice. No portion of this document may be copied, reproduced or transcribed without the expressed written consent of TotalTrax, Inc. Every effort has been made to ensure accuracy in content. However, software and hardware configurations, specifications and pricing are subject to change without notice.

All brand names, product names or trademarks appearing herein are registered to the respective companies or organizations that own the trademarks or copyrights.

TotalTrax ImpactManager® ID, TotalTrax ImpactManager® RF, TotalTrax UsageManager, TotalTrax StartManager, TotalTrax FleetControl® Manager and TotalTrax EquipManager® are trademarks of TotalTrax Incorporated in the United States.

Contents

Section 1. Introduction **1**

1.1 PC Requirements 1

1.2 Operating System Requirements 2

Section 2. Installing EquipCommand Software **3**

Section 3. Starting EquipCommand Software **11**

Section 4. System Configuration **15**

4.1 Selecting the Site in Profile and Configuration Windows 15

4.2 Software Setup Wizard 16

4.2.1 Site Setup 16

4.2.2 License Key 18

4.2.3 System-Wide Date/Time Format 19

4.2.4 E-Mail Server Configuration 19

4.2.5 Network Profiles 20

4.2.5.1 Uploading Wireless Certificates to the EquipCommand Server 23

4.2.5.2 Access Points 24

4.2.6 User Configuration 24

4.3 Unit Setup Wizard 26

4.3.1 Select Hardware Model 27

4.3.2 Unit Owners 27

4.3.3 Model and Manufacturer 28

4.3.4 Unit Profiles 29

4.3.5 Accelerometer Profiles 35
4.3.6 Unit Configuration 37
4.4 Operator Access Setup Wizard 40
4.4.1 Supervisors 40
4.4.2 Operator and Key Configuration 42
4.4.3 Work Shift Profiles 45
4.4.4 Operator Assignments 46
4.4.5 Operator Certifications 47
4.5 Event Alerts Setup Wizard 49
4.5.1 Alert Targets 49
4.5.2 Alerts and Monitoring 50
4.6 Custom Events 53
4.6.1 Event Configuration 53
4.6.2 Creating Custom Events 54
4.7 Additional Information Setup Not Covered in the Wizards 55
4.7.1 Changing Passwords and the Time Zone 55
4.7.2 Setting Up Equipment Groups 56
4.7.3 Operator Import from File 58
4.7.4 Setting Up Event Categories 59

Section 5. Using Keys 61

5.1 Accessing Units with the Green Operator Key 61
5.2 Performing a Safety Check with the Green Operator Key 61
5.3 Loading Unit Settings Using Keys 62
5.4 Manually Retrieving Events Data from a Unit 62
5.5 Performing Inspections and Lockouts with the Blue Maintenance Key 63
5.6 Resetting ImpactManager RF with the Black Resetter Key 63
5.7 Key Tools 64
5.7.1 Show Attached Keys 64
5.7.2 Assigned Keys 65
5.7.3 Blocked Keys 66

Section 6. Loading Unit Configuration Information 69

6.1 Loading Unit Configuration Information onto the Red Settings Key 69

6.2 Loading the Operators List onto the Yellow Managers Key 71
6.3 Loading the Unit Wireless Certificates onto the Orange Certificate Key 73
6.4 Loading the Unit Settings from Keys into the Unit 73
6.5 Loading Unit Configurations over the Wireless Network 74

Section 7. System Monitoring 77

7.1 Unit Status 77
7.2 Event History 78
7.2.1 Pre-Defined Event Types 79

Section 8. Reports 83

8.1 Available Reports and Charts 84
8.1.1 Events Reports 84
8.1.2 Utilization Reports 85
8.1.3 Impact Reports 86
8.1.4 Operator Certification Expiration Report 87
8.1.5 Simultaneous Utilization Report 87
8.2 Scheduled Reporting 87

Section 9. System Utilities 91

9.1 Maintenance Due Report 91
9.2 Server Trace 92
9.3 E-mailing Log Files to TotalTrax 93
9.4 Displaying System Information 94
9.5 Tool Tips 94

Section 10. Dashboard Configuration 95

Section 11. Database Backup Configuration 99

11.1 Configuring an Automated Backup of the EquipCommand Database 99

Appendix A. iButton Keys and LED Status Indications 101

A.1 iButton Key Definitions and Verification Sounds 101
A.2 iButton Reader LED Status Indications 102

Section 1. Introduction

EquipCommand is a Java™-based application used to configure, monitor, and manage the EquipManager. The application is browser-based and requires an Internet browser as a "front-end" to provide the graphical user interface (GUI). Suitable browsers are:

Firefox: version and later, free for downloading at http://www.mozilla.com/firefox/

Internet Explorer: version 7.0 and later, free for downloading at http://www.microsoft.com/windows/downloads/ie/getitnow.mspx/

1.1 PC Requirements

The minimum feature set for the hosting server is:

- Intel Core 2 (2.0 GHz or faster)
- 2 GB RAM
- 1 GB available disk space

NOTE: This can vary significantly depending on implementation details (number of users or ImpactManager RF units, other applications on the server, etc.).

The minimum feature set for the hosting PC is:

- Intel Celeron or Core 2 (1.2 GHz or faster)
- 512 MB RAM
- 10 MB of available disk space

If proximity cards or iButton keys are used for operator access, at least one workstation requires an available serial/com port or USB port.

1.2 Operating System Requirements

The EquipCommand software can be installed on any Windows operating system that supports system services.

The software can also be installed on HP-UX and Linux systems; however, special instructions will be required. If you intend to install on HP-UX or Linux, contact TotalTrax Technical Services.

Supported Microsoft® Windows® Operating Systems are:

- Windows 7 (Ultimate/Business)
- Windows Vista (Ultimate/Business)
- Windows 2008
- Windows 2008 R2
- Windows XP Pro (service pack 2)
- Windows 2003

EquipCommand can also be installed on Virtual Machines using the following utilities:

- Microsoft Virtual Server
- VMWare
- Sun VirtualBox

Section 2. Installing EquipCommand Software

Applications Installed During Installation

For Servers:

- JBoss® J2EE Application Server
- MySQL® Database
- TotalTrax Proprietary code
- Java™ 2 JDK

NOTE: The application is installed as a Windows system service.

For Workstations:

- Dallas Semiconductor iButton® drivers
- TotalTrax proprietary code

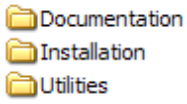
NOTE: Key writer is installed as a Windows system service.

Installing the EquipCommand Software

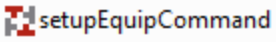
To install the EquipCommand software:

1. Insert the EquipCommand single-installation CD.

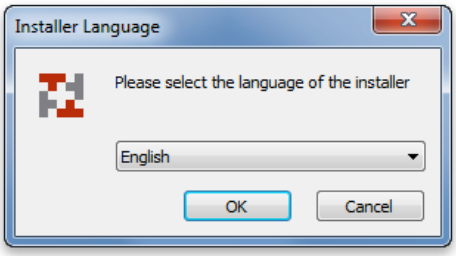
   The CD directory displays, as shown below.

2. Open the Installation folder.
3. To begin the installation, double-click the Setup.exe icon.

   You are prompted to select a language (English, French, or Spanish).



4. Select the language you want to use.

   The License Agreement window displays.

5. To accept the terms of the license agreement, click the I Agree button.

   The Select Components window displays.

By default, both the Server and Workstation components are selected to be installed.

The Server application is installed where the target PC or Server is to be the hosting hardware. Usually, the Server application is installed only on a single PC or Server.

The Workstation application is installed on the PCs or Server where the data for iButton keys will be written. Usually the Workstation application is installed on multiple PCs.

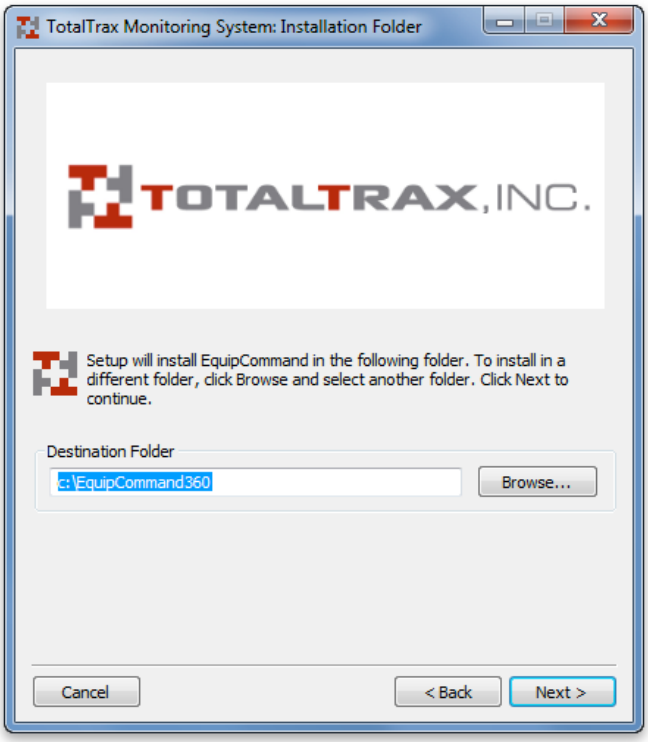
6. Use the default component selections.

   –OR-

   Select the specific components you want to install.

7. Click Next.

   You are prompted to select the folder location where the Server and Workstation application will be installed.



8. Use the default folder.

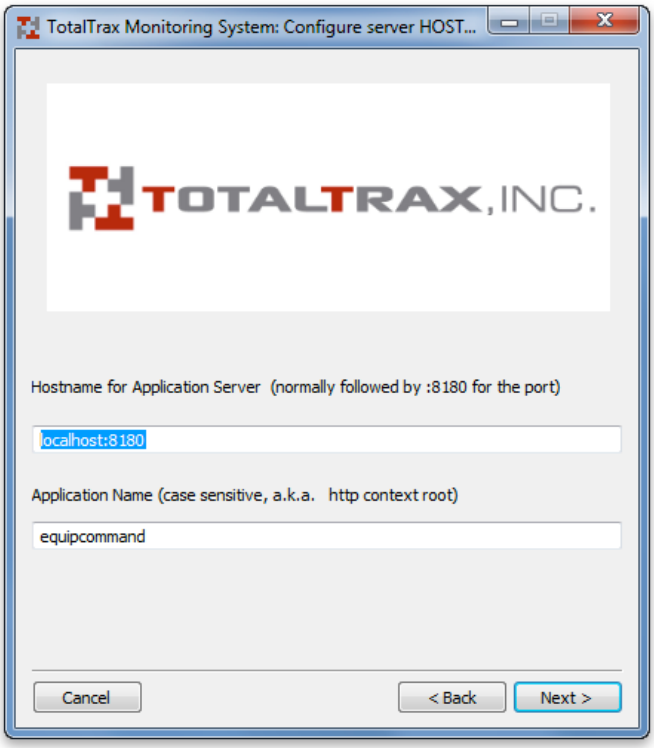
   -OR-

   Click the Browse button, then navigate to the folder you want to use and select it.

9. Click the Next button.

   You are prompted to enter the host name and TCP port for the Server application.

   The default name is **localhost** and the default TCP port on which the application will communicate is **8180**.



10. Accept the default host name and TCP port.

    -OR-

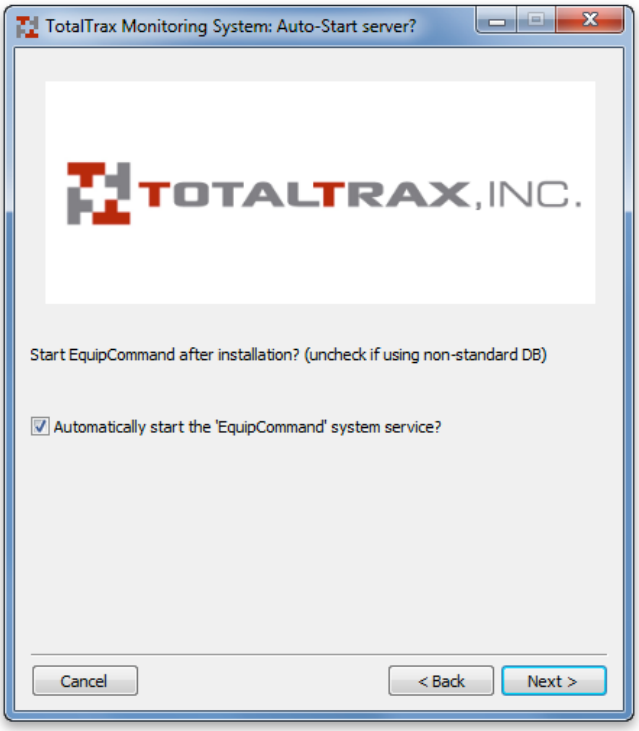
    Enter a different host name and/or TCP port.

    If you are installing only on a workstation that will be remotely accessing the host PC or Server, you will not use the default hostname. You must enter either the DNS name or the IP address of the Server and the TCP port on which the Server is listening. Examples include:

    - Networkserver:8180
    - 27.14.221.17:8180
    - Click the Next button.

    If you chose to install the Server software, you are prompted to start the server service automatically or manually.

NOTE: If you choose to start the service manually, remember that if the service is not running, no data will be collected.



11. To have the EquipCommand server software start automatically after installation is complete, select the Automatically Start option.

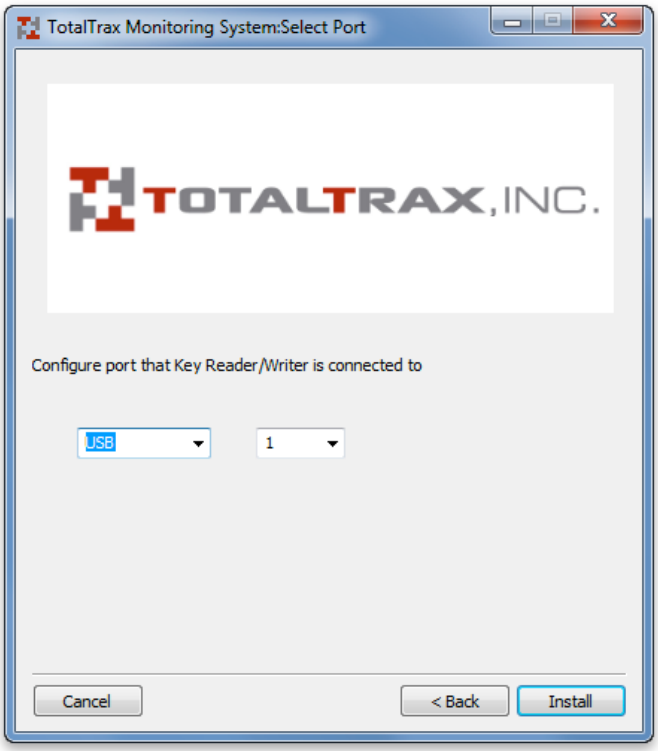
    - OR -

    If you are using a non-standard database, clear the Automatically Start option.

12. Click the Next button.

    The Select Port window displays. This window is used to install the drivers that support the iButton key readers, should you want to use the iButton function.

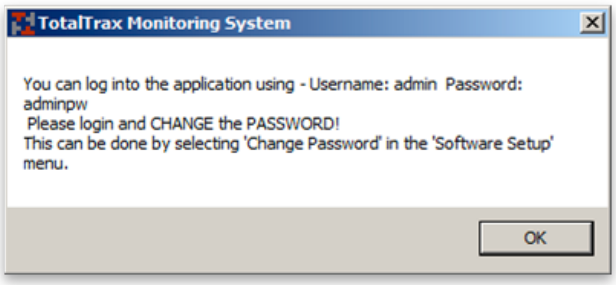
NOTE: To correctly install these drivers, you must physically connect the key reader hardware to your PC or Server. There are two pieces of hardware required: the Microlan cable (blue dot reader) and the LPT, serial, or USB adapter.



13. Select the reader type connection (LPT, serial, or USB) to be used.
14. Click the Install button.

    The software installation process begins.

    During the installation, a prompt displays that indicates the default username and password to use to log into the application. You are reminded to change the password from the default value as soon as possible to secure the system.



15. Make a note of the username and password, then click the OK button to dismiss the password prompt.

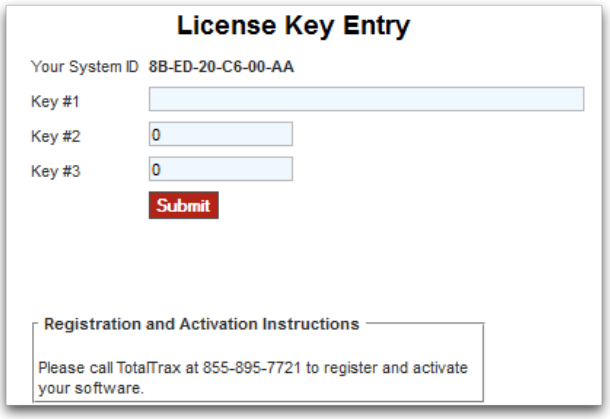
    The installation continues. A prompt indicates when the installation is finished.

Software Activation Keys

Upon the first use of the EquipCommand software, you are prompted to call TotalTrax, Inc. Technical Support at (855)-895-7721 to obtain your activation keys.

Technical Support business hours are 7:00 a.m. to 5:00 p.m. CST, Monday - Friday. Activation keys are issued by TotalTrax, Inc. to enable the EquipCommand software.

If a user logs in and the activation keys have not been applied, the activation window displays. The software will permit usage under a temporary key for a period of ten days from the installation date.



NOTE: To add a TotalTrax hardware product to be managed by the EquipCommand software after initial installation, obtain the required license keys from TotalTrax, Inc. Then, in the System Setup menu in the menu bar, click License Key Entry. The License Key Entry window shown above displays. Enter the license keys.

Section 3. Starting EquipCommand Software

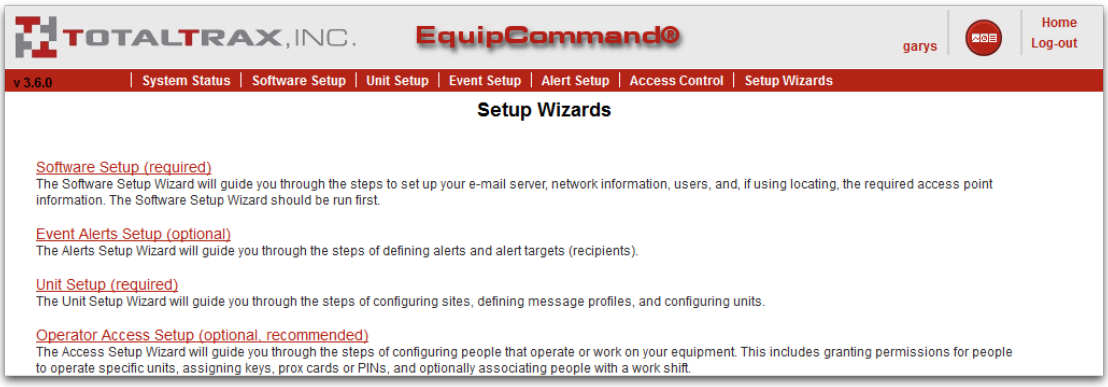
To start the EquipCommand software:

1. Double-click the TotalTrax Login icon on your PC desktop.

   The initial Login window displays. The default Username is **admin** and the default password is **adminpw**.

2. In the appropriate fields, enter the username and password you want to use, then click the Log-in button.

   The home page displays.



The main EquipCommand menus are displayed in the red menu bar across the top of the home page. These menus include:

- System Status
- Software Setup
- Unit Setup
- Event Setup
- Alert Setup
- Access Control
- Setup Wizards

In addition to the menus, the home page also includes links to the Setup Wizards to help you get started, fast. The Setup Wizards include:

- Software Setup (required)
- Unit Setup (required)
- Operator Access Setup (optional, recommended)
- Event Alerts Setup (optional)

NOTE: Each of the setup windows in the Setup Wizards can also be accessed directly using the menus in the menu bar. In the procedures in this manual, the appropriate menu options are provided.

The EquipCommand Software is structured to allow the user extensive means to configure the application to best fit the specific needs. The next five sections describe the configuration and other tasks:

- System Configuration reviews the process by which specific information regarding unit function, equipment, operators, etc. is entered into the software. The process is presented in logical order and it is highly recommended that you follow this order. Otherwise, you may encounter situations where you desire to enter specific information but the software will not allow you to do so until other information is selected and/or entered. It is recommended that you follow the Setup Wizards located on the home page when first setting up the system to

ensure all information is entered in the correct order. All Setup Wizards are also accessible from the Setup Wizards menu.

- Using Keys describes keys, which are the primary interface between the EquipCommand software and the ImpactManager RF unit.
- System Monitoring describes how to review the current status of the software and the units that are being monitored.
- Data Review describes how to review and organize data received from the units being monitored. You are also instructed on how to produce reports, tables, and graphs of your data.
- System Utilities describes how to use various tools and features supported by the software that are not detailed in other sections.

Section 4. System Configuration

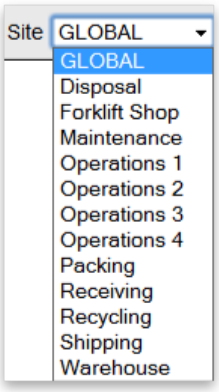
System configuration includes setting up the following components:

- Software
- Units
- Operator access
- Operators
- Event alerts
- Custom events

4.1 Selecting the Site in Profile and Configuration Windows

If you have multiple sites configured in the EquipCommand system, many of the profile and configuration windows allow you to specify settings globally or by site.

Use the list at the upper right corner to specify which site you are defining the settings for.



For more information about setting up sites, refer to "Site Setup" on page 16.

4.2 Software Setup Wizard

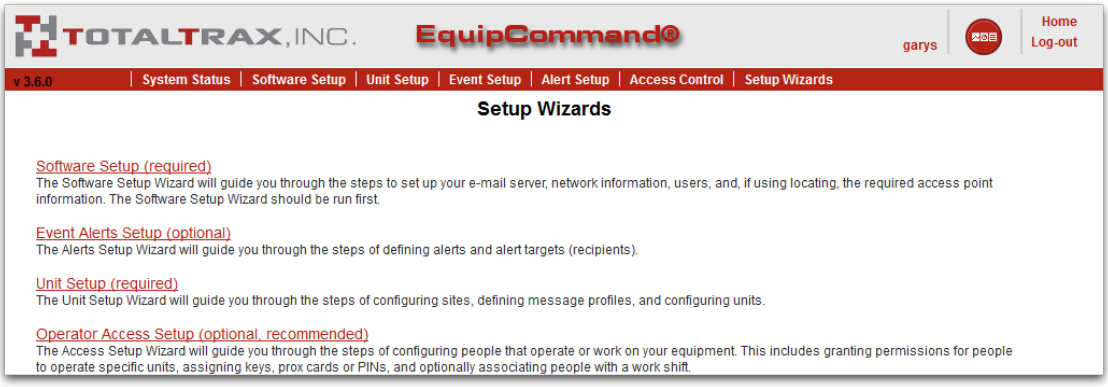
The Software Setup Wizard guides you through the process of setting up:

- Site profiles
- The license key
- The date/time format to use throughout the system
- E-mail server configuration
- Network profiles
- User configuration

NOTE: Run the Software Setup Wizard first, before running the other Wizards.

To run the Software Setup Wizard:

1. Click the Software Setup link on the home page.



   The Wizard starts and the first Software Setup window displays.

2. Complete the fields and options in each window, as needed.

   For detailed procedures, refer to the next subtopics.

3. To advance to the next step within the Wizard, click Next Step.

   To go back a step, click Prev Step.

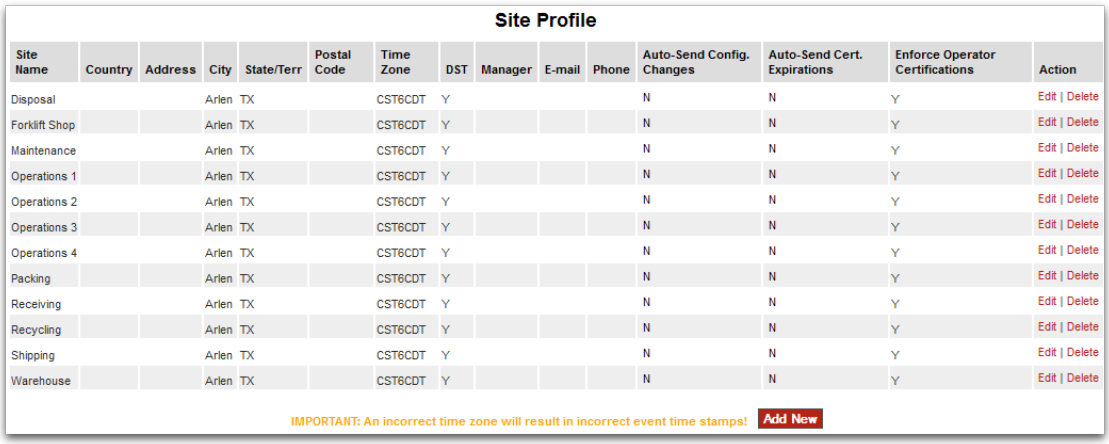
4.2.1 Site Setup

The EquipCommand software can manage units operating at various locations. These locations, or sites, must be identified. Operators, supervisors, and units can be assigned to specific sites. In addition, specific EquipCommand software users can be designated to view site-specific information (for example, supervisors in Dallas can be limited to viewing/changing data specific to the Dallas site, rather than company-wide).

To set up a site:

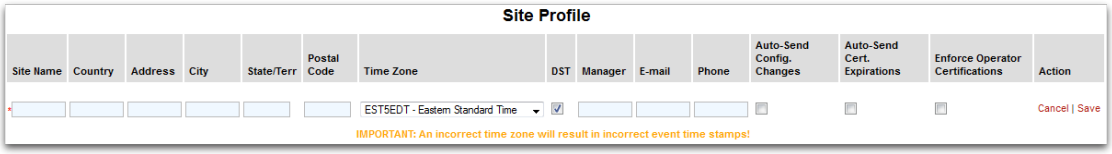
1. If you are not using the Software Setup Wizard, in the Unit Setup menu, click Site Profile.

   The Site Profile window displays.



2. To add a site, click the Add New button.

   The Site Profile - Add New window displays.



3. Complete the fields and options to set up the site.

   Refer to the following tables for a description of the fields and options.

NOTE: If you want to manage multiple sites within a single EquipCommand software installation, at least one user should be assigned All Site Access capabilities. For information about assigning a user access to sites, refer to "User Configuration" on page 24.

Site Profile Fields and Options	Description
Site Name	Required. The login username for the user.
Country, Address, City, State/Terr, Postal Code	The user's address information.
Time Zone	Required. The site's time zone.
DST	Select this check box if the site uses Daylight Savings Time.

Site Profile Fields and Options	Description
Manager	The manager at the site.
E-mail	The manager's e-mail.
Phone	The manager's phone number.
Auto-Send Config Changes	When this option is selected, the software will automatically send profile changes to affected units when changes are made to unit settings (provided that the unit is communicating wirelessly with the server).
Auto-Send Cert. Expirations	When this option is selected, the software will automatically send Forklift Certification expiration dates. If the Enforce Operator Certifications setting is not enabled, this feature will not be used.
Enforce Operator Certifications	When this option is selected, only operators with a valid certification (within EquipCommand) can log in to units. **NOTE:** Do not enable this option until all certifications have been entered into EquipCommand.

4. When finished, click the Save link in the Action column to add the site.

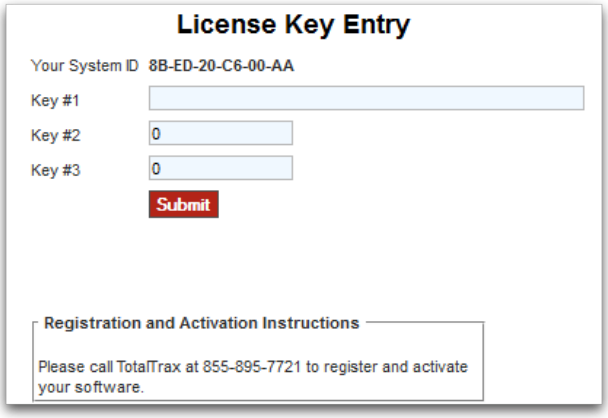
4.2.2 License Key

The license key is typically added during EquipCommand software installation, which prompts you for the key at the completion of the install process.

If you need to add a license key for a TotalTrax product:

1. If you are not using the Software Setup Wizard, in the Software Setup menu, click License Key Entry.

   The License Key Entry window displays.



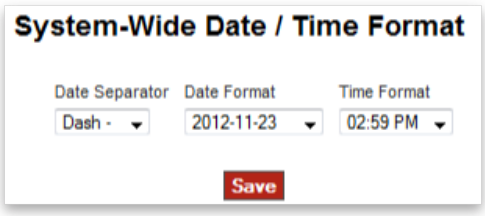
2. Enter the license key and the click the Submit button.

4.2.3 System-Wide Date/Time Format

To set the date and time format to be used throughout the system:

1. If you are not using the Software Setup Wizard, in the Software Setup menu, click Date/Time Format.

   The System-Wide Date/Time Format window displays.



2. Select the separator character for the date, the date format, and the time format.
3. When finished, click the Save button to save the format settings.

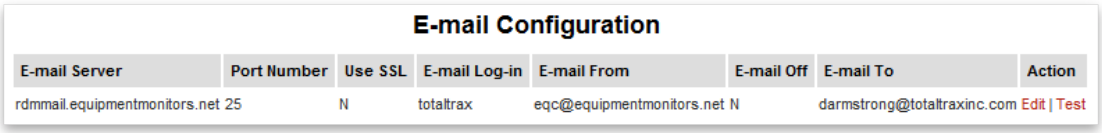
4.2.4 E-Mail Server Configuration

To support EquipCommand e-mail messaging, the EquipCommand software must be configured to with information about the e-mail server that is going to be used.

To configure the e-mail server:

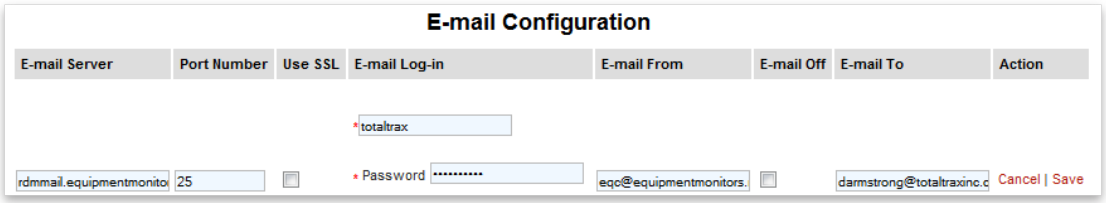
1. If you are not using the Software Setup Wizard, in the Software Setup menu, click Email Configuration.

   The E-mail Configuration window with the default settings displays.



2. To change the default settings to values that work with your local e-mail server, click the Edit link in the Action column.

   The E-mail Configuration – Edit window displays.



3. Update the fields in the window to change the settings, as needed.

Refer to the table below for a description of the fields.

E-Mail Configuration Field	Description
Mail Server	The local e-mail server being used.
Port Number	The port number for the e-mail server.
Use SSL	Select this option if you are using Secure Sockets Layer (SSL) to secure communications between EquipCommand and the e-mail server.
E-mail Log-in	The login name for the EquipCommand e-mail account.
Password	The password for the EquipCommand e-mail account.
E-mail From	The e-mail address used for outgoing EquipCommand e-mails.
E-mail Off	Select this option to disable the e-mail messaging feature.
E-mail To	The e-mail address used for incoming EquipCommand e-mails.

4. When finished, click the Save button in the Action column to save the updated configuration settings.

4.2.5 Network Profiles

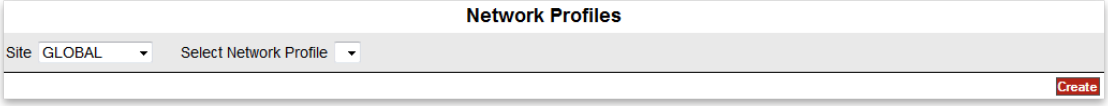
The ImpactManager RF unit uses an 802.11b wireless module to relay data to your network. The 802.11b format requires that you provide specific information about your wireless network so that the EquipCommand software can connect to and communicate with it. Network information is provided to the EquipCommand software through the use of Network profiles.

NOTE: If you are using the WPA2 PEAP, TLS, or TTLs wireless security methods, wireless certificates for the units using this Network profile must be uploaded to the EquipCommand server before configuring the profile. For instructions, refer to "Uploading Wireless Certificates to the EquipCommand Server" on page 23.

To create a Network profile:

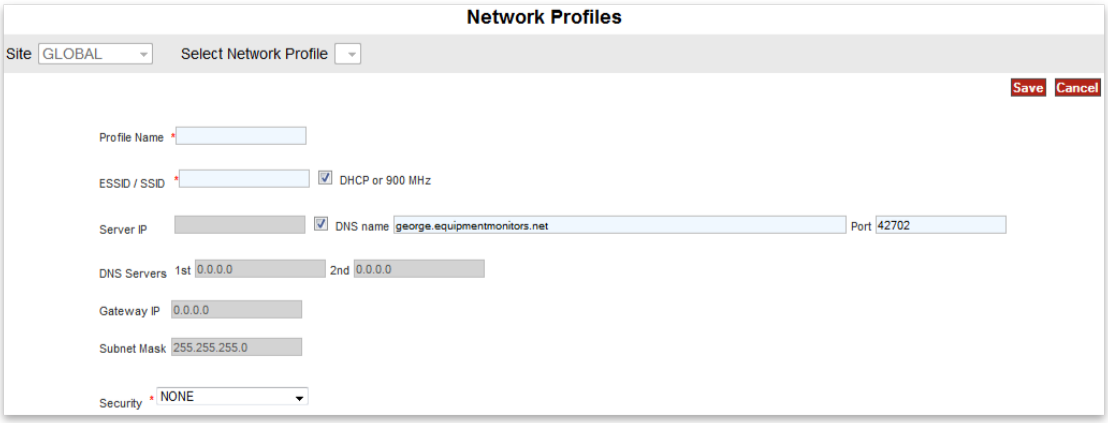
1. If you are not using the Software Setup Wizard, in the Software Setup menu, click Network Profiles.

   The Network Profiles window displays.



2. Click the Create button.

   The Network Profiles - Add New window displays.



3. Complete the fields and options in the window to set up the new Network profile.

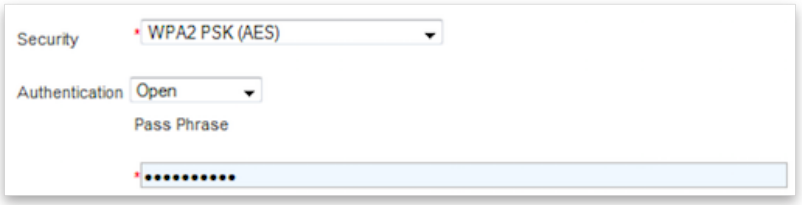
   Refer to the table below for a description of the fields and options.

Network Profile Fields and Options	Description
Profile Name	Enter the name of the Network profile.
ESSID/SSID	Enter the identifying name of the target wireless network.
DHCP or 900 MHz	Select this option if you are using 900-MHz RF or a Wi-Fi network and DHCP (dynamic host configuration profile) to communicate with units. If you are using Wi-Fi and are manually entering the IP address information, then clear this option.
Server IP	Enter the server IP address or its DNS-recognized name.
DNS name	If DHCP is selected and you want to have IP addresses automatically assigned by the DNS (domain name system) server to the units rather than manually entering them, select this check box and enter the name of the DNS server.
Port	The default port number for EquipCommand is 42768.
DNS Server 1st/2nd	Enter the IP address of the DNS servers that are providing DNS resolution. If your network supports DNS and you have used the DNS name to identify either or both the Primary Server and Secondary Server, you must specify the IP address of your DNS Servers. If you are not using DNS, no information needs to be entered.
Gateway IP	Enter the IP address of your network's gateway to the Internet or to another network.

Network Profile Fields and Options	Description
Subnet Mask	Enter an IP address grouping structure for the target network.
Security	If using wireless security, select the wireless security method. **NOTE:** The proper security method must be selected for ImpactManager RF to be able to communicate on the wireless network. Please verify the security method for your network before selecting the wireless security method.

Depending on the security method you select in the Security list, additional security configuration fields and options display, as shown below.

NOTE: Configuring wireless security modes will require IT involvement to ensure that all appropriate settings are selected and configured.



4. Complete the fields and options for the security mode you selected.

   Refer to the table below for a description of the fields and options for each security mode.

Wireless Security Field	Security Types to Which Field Applies	Description
Authentication	All	Select the authentication method for the wireless network.
Key#	WEP	The key number being used.
WEP Key	WEP	For WEP: • Enter 10 hexadecimal digits for each 40/64 WEP key • Enter 26 hexadecimal digits for 104/128 WEP key
Username and Password	LEAP WPA2 PEAP WPA2 TLS WPA2 TTLS	The wireless access username and password.

Wireless Security Field	Security Types to Which Field Applies	Description
Pass Phrase	WPA (all) WPA2 PSK (all)	The wireless access pass phrase. For WPA2 PSK pre-calculated, the pass phrase is hex only.
Use .P12 /.PFX certificates	WPA2 TLS	Select this option if you are using .p12 or .pfx encrypted certificate file formats.
Advanced Options	WPA2 PEAP WPA2 TLS WPA2 TTLS	Advanced options for these security types. **NOTE:** These options are not typically used. Contact TotalTrax Technical Support if you believe you need to use these options.
CA Cert	WPA2 PEAP WPA2 TLS WPA2 TTLS	Select the CA certificate.
Client Cert	WPA2 TLS	Select the client certificate.
Private Key	WPA2 TLS	Select the private key.

5. When finished, click the Save button to save the new Network profile.

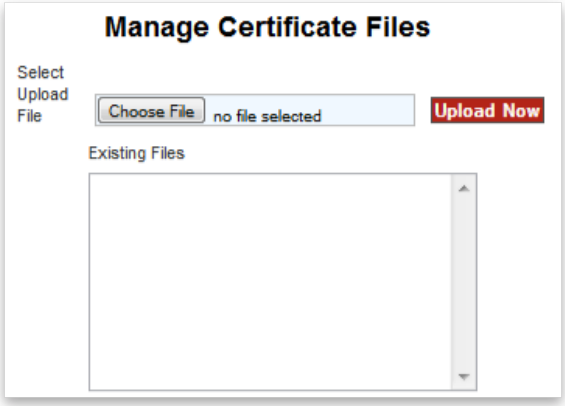
4.2.5.1 Uploading Wireless Certificates to the EquipCommand Server

The WPA2 PEAP, TLS, and TTLs wireless security methods require that each unit has wireless certificates to properly authenticate access to the wireless network. The wireless certificates used by your site must be uploaded to the EquipCommand server so that they can be selected in the Network Profile window when the wireless security method is being configured.

To upload a wireless certificate:

1. In the Software Setup Menu, click Manage Certificate Files.

   The Manage Certificate Files window displays.



2. To select the certificate to be uploaded, click the Choose File button.

   A browse window displays.

3. Browse to your certificate file and select it, then click the Open button.

   The certificate name is displayed in the Select Upload File field.

4. To upload the selected certificate, click the Upload Now button.

   The new wireless certificate uploads and is listed in the Existing Files box.

For the procedure on how to select the certificates for a security method, refer to "Network Profiles" on page 20.

For procedures on how to load the certificates into a unit, refer to "Loading the Unit Wireless Certificates onto the Orange Certificate Key" on page 73 and "Loading the Unit Settings from Keys into the Unit" on page 73.

4.2.5.2 Access Points

ImpactManager RF does not support locating functionality. When using the Software Setup Wizard, click the Next Step button to move the next setup window.

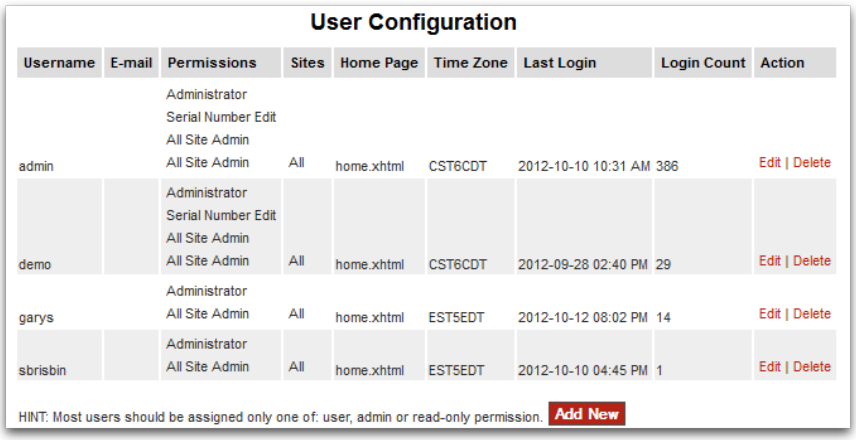
4.2.6 User Configuration

> **NOTE:** This procedure is available only to users who have logged in as an Administrator.

To configure a user:

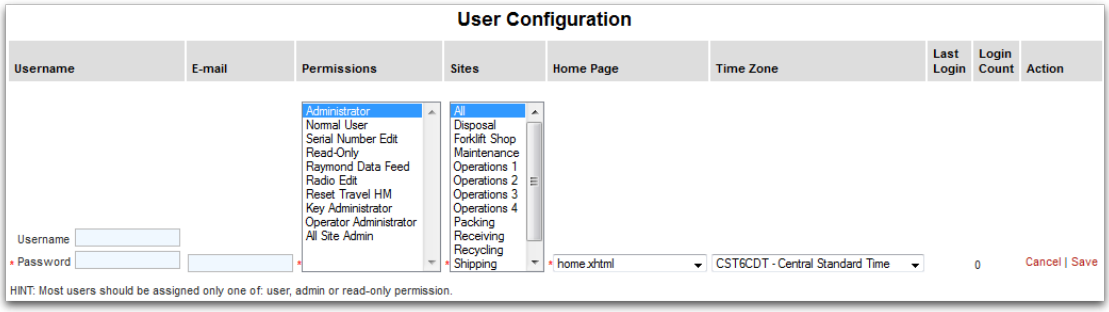
1. If you are not using the Software Setup Wizard, in the Software Setup menu, click User Configuration.

   The User Configuration window displays.



2. To add a user, click the Add New button.

   The User Configuration - Add New window displays.



Refer to the following tables for a description of the fields and options.

User Configuration Fields and Options	Description
Username	The login username for the user. **NOTE:** Spaces are not allowed in the username.
Password	The login password for the user.
E-mail	An identifier for the login account name.
Permissions	Select one or more permissions for the user. You can Ctrl+click to select multiple permissions. For a description of user permission levels, refer to the next table.
Sites	Select the sites to which the user will have access. Ctrl+click to select multiple sites. Users can access, view, or change only sites assigned to their login.
Home Page	The default page that is displayed for this user after logging in.
Time Zone	Select the time zone to use for the times that are displayed throughout the EquipCommand user interface.
Last Login	Time stamp that indicates when this user was last logged into EquipCommand.
Login Count	The number of times this user has logged into EquipCommand.

3. Enter the username in the Username field and the user password in the Password field.
4. From the Permissions list, select one or more permissions for the user.

   Ctrl+click to select multiple permissions.

   Refer to the table below for a description of the user permission levels.

User Permission Level	Description
Administrator	Individual Site Access. Full access to all windows and settings within their given site. Should be reserved for TotalTrax system administrators.
Normal User	Individual Site Access. Access to most windows. Ability to add operators and keys, run reports, and configure keys. User cannot delete items from the database.
Serial Number Edit	Individual Site Access. Adds the ability to delete serial numbers from the software. Only used when replacing or moving hardware.
Read Only	Individual Site Access. User has access to all windows, but cannot add or modify any information in the software. Can generate reports.
Key Admin	Individual Site Access. User has access to Operator and Key Configuration (for adding Operators), Blocked Keys, Assigned Keys, Attached Keys, Write Configuration Key for Unit, and Send Configuration via Radio. No access is given to any other software window.
Operator Admin	Individual Site Access. User has access to Operator and Key Configuration (for adding Operators), Blocked Keys, Assigned Keys, Attached Keys, and Send Configuration via Radio (to send Operators Lists only).
All Site Access	Multi-Site Access. User has access to all sites within the EquipCommand Server.

5. When finished, click the Save link in the Action column to add the user.

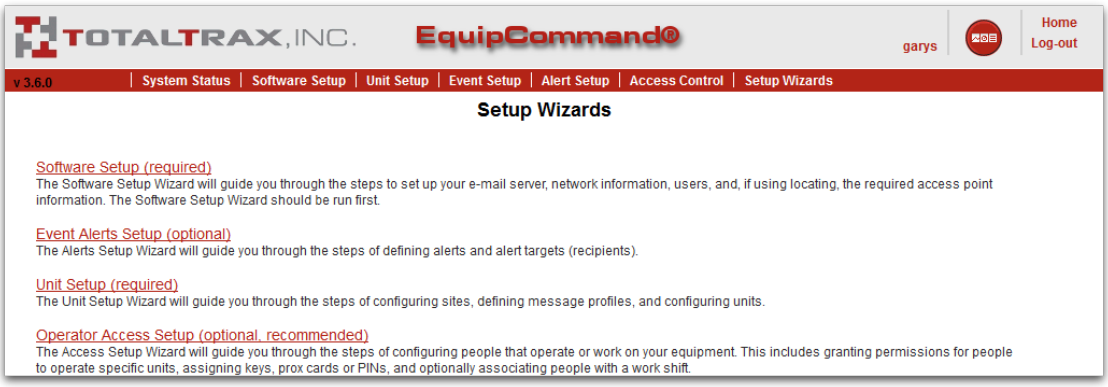
4.3 Unit Setup Wizard

The Unit Setup Wizard guides you guides you through the process of setting up units, including:

- Hardware model
- Unit owner
- Model and manufacturer
- Unit profiles and Accelerator profiles
- Unit configuration

To run the Unit Setup Wizard:

1. Click the Unit Setup link on the home page.



The Wizard starts and the first Unit Setup window displays.

2. Complete the fields and options in each window, as needed.

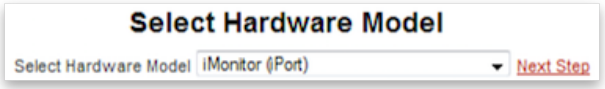
   For detailed procedures, refer to the following topics.

3. To advance to the next step within the Wizard, click Next Step.

   To go back a step, click Prev Step.

4.3.1 Select Hardware Model

The first Unit Setup wizard window prompts you to select the unit's hardware model.



Select the unit's hardware model in the list and then click the Next Step link.

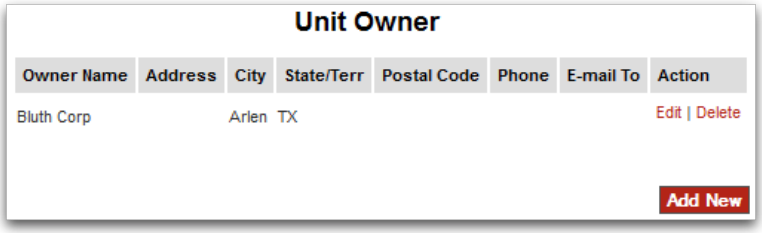
4.3.2 Unit Owners

Entering unit owner information is optional. This information is used for data filtering in certain EquipCommand functions and to provide contact information. The information applies to situations in which the owner of particular equipment is different from the user, such as in a leasing scenario.

To set up Unit Owner information:

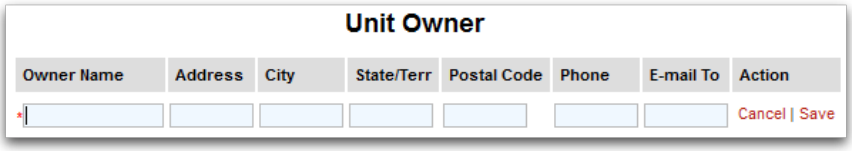
1. In the Unit Setup menu, click Owners.

   The Unit Owner window displays.



2. To add a new Unit Owner, click the Add New button.

   The Unit Owner - Add New window displays.



3. In the corresponding fields, enter the owner name, address, phone number, and e-mail address.
4. When finished, click the Save link in the Action column to save the new Unit Owner.

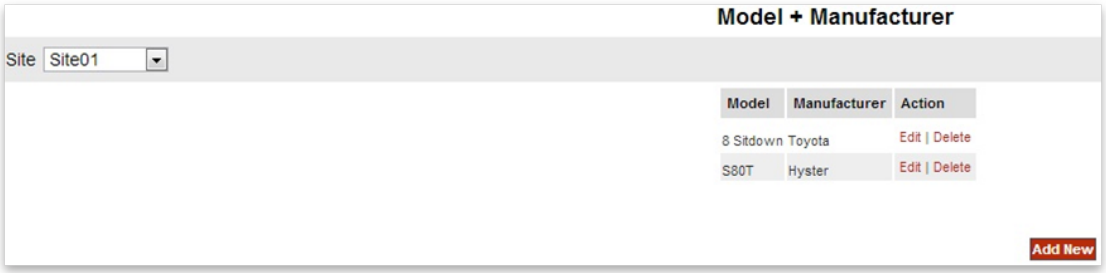
4.3.3 Model and Manufacturer

Entering model and manufacturer information is optional. This information is used only for data filtering in certain EquipCommand functions.

To add model and manufacturer type information:

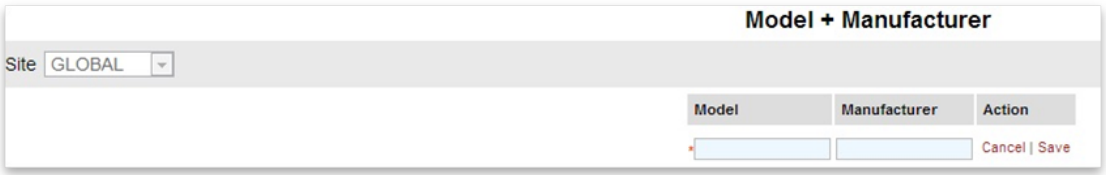
1. In the Unit Setup menu, click Model Types.

   The Model + Manufacturer window displays.



2. To add a new Model and Manufacturer entry, click the Add New button.

   The Model + Manufacturer - Add New window displays.



3. Enter the model and manufacturer information.

   Refer to the following table for a description of the fields and options.

Model Fields and Options	Description
Model	Name of the model.
Manufacturer	Name of the model manufacturer.

4. When finished entering the information, click the Save link in the Action column to add the Model and Manufacturer entry.

4.3.4 Unit Profiles

The EquipCommand software allows you to create Unit Profiles. Each Unit Profile controls and defines how a particular unit functions. A single Unit Profile can be used for all units or for groups of units, or a specific Unit Profile can be created for individual units.

NOTE: If you want all of your units to function exactly the same, you do not need to create more than one Unit Profile.

The configuration settings for Unit Profiles determine the actual functioning of the unit being programmed.

NOTE: There are many configuration settings. It is very important to understand each configuration setting, as a wrong setting will result in the unit not functioning as expected.

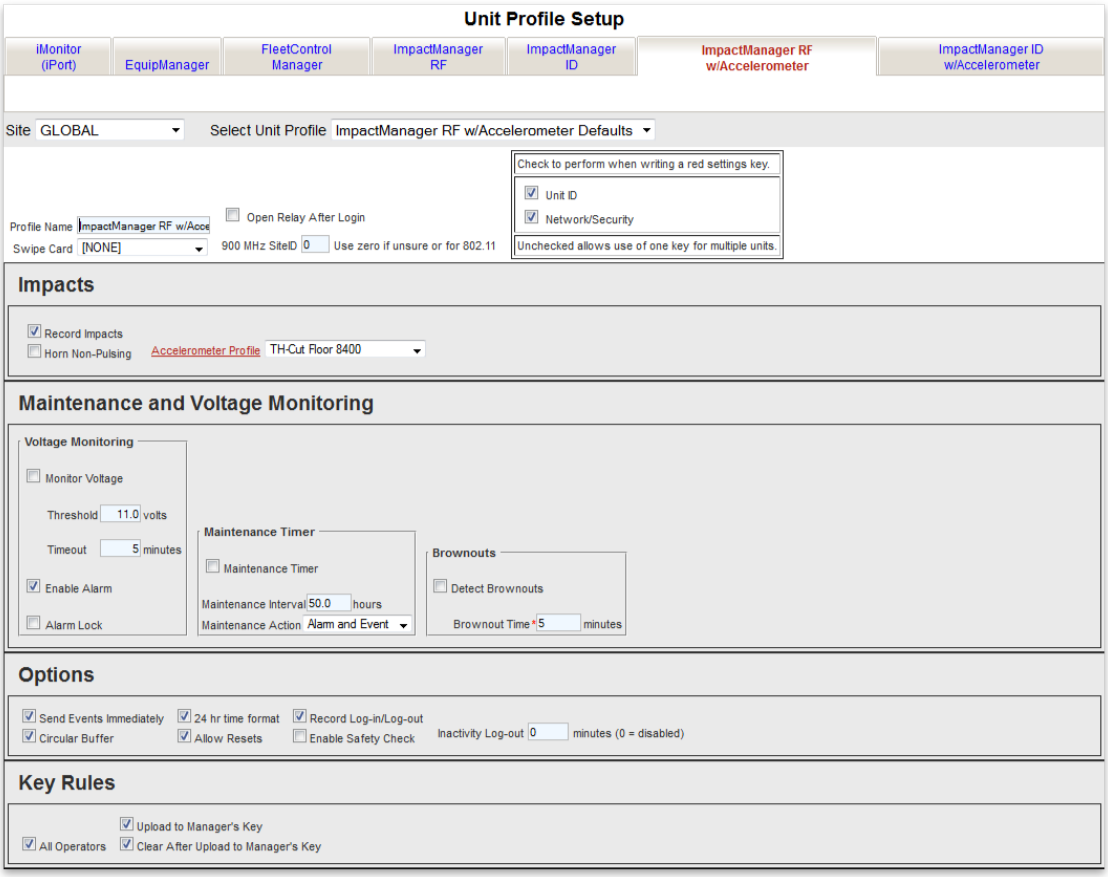
To set up a Unit Profile:

1. If you are not using the Unit Setup Wizard, in the Unit Setup menu, click Unit Profiles.

   The Unit Profile Setup window displays.

   The Unit Profile Setup includes tabs for each of the EquipCommand Managers.

2. Go to the ImpactManager RF tab.



3. Create a new profile and then complete the fields in the window to set it up.

   For detailed procedures, refer to the following topics.

4. When finished, click the Save button to add the profile.

Creating or Modifying a Unit Profile

The default Unit Profile is labeled as ImpactManager RF defaults.

If you intend to have all your units function the same, simply edit the settings for the ImpactManager RF Defaults profile.

If you intend to create specific profiles types of units or groups of units, create a new profile.

To create a new profile:

1. From the Unit Profile Setup window, click the Create button.
2. In the Profile Name field, enter the name of the new profile.
3. Enter any additional information required, as detailed in the following topics.
4. When finished, click the Save button to create the Unit Profile.

Swipe Card

In the Swipe Card list, select the card reader that is being used. If only the standard iButton reader is used, select the default value of (NONE).

Open Relay After Login

NOTE: This option is not used.

Check to Perform When Writing a Red Settings Key

To update the unit settings when a Red key is programmed for the unit, select Unit ID check box option.

To update the network/security settings when a Red key is programmed for the unit, select Network/Security check box option.

If the check box is cleared, the settings will not be updated when the unit is programmed with a Red key.

Impacts Settings

The following table describes the Impacts settings.

Impacts Settings	Description
Record Impacts	By default, ImpactManager RF is programmed to sense and respond to impacts. If you do not want ImpactManager RF to sense impacts, clear this check box.
Horn Non-Pulsing	Select this option to have ImpactManager RF sound the horn continuously. If this option is not selected, ImpactManager RF will cause the horn to pulse at 1-second intervals.
Accelerometer Profile link	A shortcut link to the Accelerometer Profile window, from which you can define the accelerometers that can be used with units. For information about setting up an Accelerometer Profile, refer to "Accelerometer Profiles" on page 35.
Accelerometer list	Select the accelerometer for this unit.

Maintenance and Voltage Monitoring

The following table describes the Maintenance and Voltage Monitoring settings.

Maintenance Setting	Description
Monitor Voltage	ImpactManager RF features a voltage monitor that allows you to track and react to the voltage supplied by the equipment. To enable this function, select this option.
Threshold	The actual voltage value being monitored.
Timeout (Minutes)	The duration of time that the monitored voltage must be less than the threshold before a trigger occurs. Once a trigger occurs, an event is automatically generated.
Enable Alarm	In addition to the event being generated, once a trigger occurs, you can select this check box to have an audible alarm on the unit itself begin sounding. This alarm will stop sounding when the voltage returns to acceptable levels.
Alarm Lock	Select this option to lock the voltage alarm so that it will continue to sound even if the voltage returns to acceptable levels. The alarm lock can be reset with the Black key.
Maintenance Timer	ImpactManager RF utilizes a motion sensor to determine when the equipment that it is monitoring is active. The cumulative results of this recorded time can be utilized as a maintenance timer. To enable this timer, select this check box.
Maintenance Interval	If the Maintenance timer is enabled, set an expiration time. At this expiration time, the timer can generate an alarm, an event, or both.
Maintenance Action	Select the action that the expiration of the Maintenance Timer generates. The choices are: • Event. A Maintenance Due event is generated. • Alarm. ImpactManager RF will begin chirping twice every 10 seconds. • Both. An Event and an Alarm will be generated.

Maintenance Setting	Description
Detect Brownouts	ImpactManager RF supports a "brownout function" for which a power disconnect to the unit can be detected. Upon detection of a brownout, ImpactManager RF will log off an operator when power is returned. This prevents another operator from using the unit when the previous operator is already logged in. Select this option to enable the brownout detection and have the previous operator automatically logged off when power is restored.
Brownout Time	The setting is used if the Detect Brownouts option is selected. This setting is the number of minutes that has to transpire before the system determines that a brownout condition has occurred. • If the unit loses power for a period of time greater than the Brownout Time, then a unit brownout will be determined to have occurred and the operator will be automatically logged out when power is restored. • If the unit power has only temporarily lost power and it is restored before the Brownout Time has transpired, the operator can continue using the unit without having to log in again. For example, if the Brownout Time is set to 2 minutes and power is lost for only 1 minute, the operator is not logged off when power is restored. **NOTE:** If the Brownout Time is set to 0 minutes and a brownout occurs, a Brownout event will be generated but the operator will not be logged off.

Options

The following table describes the Options settings.

Options Setting	Description
Send Events Immediately	Select this option to have ImpactManager RF send events as they are generated. If this option is cleared, ImpactManager RF will accumulate 10 events prior to sending them. An impact event forces an immediate send regardless of how many events are accumulated.
Circular Buffer	Select this option to enable the circular buffer method for storing events. ImpactManager RF can store up to 500 events in its memory. Should this memory become full, there are two memory management methods that can be used. • The default method is to maintain the first 499 events and then keep event 500 as the most recent event. • The circular buffer method "cycles" the memory so that the most recent 500 events are maintained.

Options Setting	Description
24-hour time format	ImpactManager RF can operate in either 12-hour or 24-hour mode. To use 24-hour mode, select this option.
Allow Resets	Select this option to enable the Black Reset key. Normally the Yellow Manager key is used to reset the alarm or the "halt on impact" mode. A Black Reset key can also be used for this function. **NOTE:** If you do use the Yellow Manager key for resets, be aware that you might inadvertently change a setting on the unit because the Yellow Manager key also carries the Safety Checklist data.
Record Log-in/Log-out	Select this option to enable the ImpactManager RF to record all operator log-in and log-out activity.
Enable Safety Check	Select this option to have ImpactManager RF record safety check events. Inserting and holding the Operator's Key in the user interface port for five seconds generates a safety check.
Inactivity Log-out	Using the same motion sensor that is used for the Maintenance Timer, ImpactManager RF can sense if the equipment is inactive for extended periods of time. The Inactivity Log-out setting determines the period of inactive time that can occur before ImpactManager RF automatically logs an operator off. The purpose of this function is to safeguard against situations when an operator leaves a piece of equipment enabled for operation. An operator should always log ImpactManager RF out when they intend to leave the equipment. The Inactivity Log-out setting acts to remedy the situation when an operator fails to do so. Set the time value from 1 to 99 minutes. A setting of 0 will disable this function.

Key Rules

The Key Rules settings allow you to specify operator access to the unit, and behavior of data uploads with the Yellow Managers key.

The following table describes the Key Rules settings.

Key Rules Setting	Description
All Operators	Select this option to have the unit accept all Green Operator keys. If this option is cleared, only the keys of those operators who have been assigned access to the unit will be accepted.
Upload to Manager's Key	Select this option to allow uploading of data to the Yellow Managers key.
Clear After Upload to Manager's Key	Select this option to have event data cleared from the unit when the Yellow Managers key is used to collect data.

For information about assigning keys to operators and assigning operator access to units, refer to "Operator and Key Configuration" on page 42 and "Operator Assignments" on page 46.

4.3.5 Accelerometer Profiles

ImpactManager RF supports the use of an internal accelerometer for detecting impacts to the vehicle being monitored. To use this option, you must create an Accelerometer profile that defines how the accelerometer will be used. You can then assign this Accelerator profile to the appropriate units in the Units Profile window (refer to "Unit Profiles" on page 29).

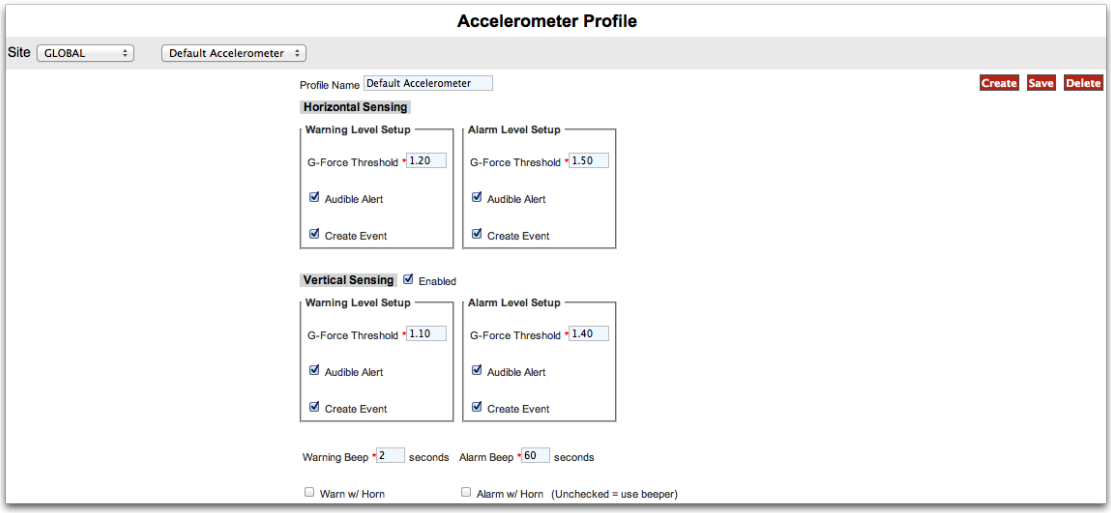
To create an Accelerometer profile:

1. From the Unit Profiles window, click the Accelerometer Profiles link.

   - OR -

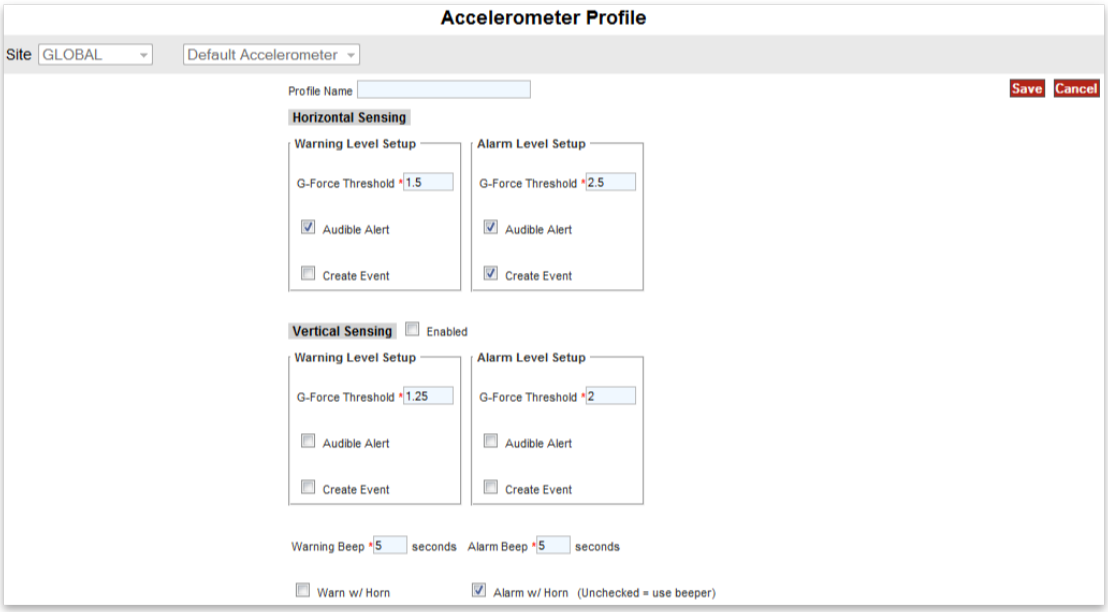
   In the Unit Setup menu, click Accelerometer Profile.

   The Accelerometer Profile window displays.



2. To create an Accelerometer Profile, click the Create button.

   The Accelerometer Profile – Add New window displays.



You can set two separate impact thresholds for both horizontal impacts (XY Plane) and vertical impacts (Z Plane).

The lower threshold is called Warning Level and the upper threshold is called Alarm Level. For each threshold, you can select the G-Force Threshold sensitivity and the actions to be taken when the threshold is exceeded.

3. To specify these settings and others for the new Accelerometer Profile, complete the fields and options in the window.

   The following table describes the fields and options.

Accelerometer Profile Fields and Options	**Description**
G-Force Threshold (Warning Level)	Enter any threshold value ranging between 0.10 G to 10.0 G. **TIP:** The Warning Level G-Force Threshold must always be set to a value less than the Alarm Level G-Force Threshold.
Audible Alert (Warning Level)	Select this option to have the ImpactManager RF piezo alarm sound when the Warning Level G-Force Threshold is exceeded. The piezo alarm will sound for the time period determined by the Warning Beep option.
Create Event (Warning Level)	Select this option to have ImpactManager RF record an event labeled "Impact - Warning" when the Warning Level G-Force Threshold is exceeded. This event will detail the time of the event and will display the peak value of the impact.

Accelerometer Profile Fields and Options	Description
G-Force Threshold (Alarm Level)	Enter any threshold value ranging between 0.10 G to 10.0 G.
Audible Alert (Alarm Level)	Select this option to have the ImpactManager RF piezo alarm will sound when the Alarm Level G-Force Threshold is exceeded. The piezo alarm will sound for the time period determined by the Alarm Beep control.
Create Event (Alarm Level)	Select this option to have ImpactManager RF record an event labeled "Impact - Alarm" when the Alarm Level G-Force Threshold is exceeded. This event will detail the time of the event and will display the peak value of the impact.
Vertical Sensing Enabled	Select this check box to enable monitoring of vertical impacts.
Warning Beep	Enter the number of seconds to sound the warning beep. The range of valid values is from 1 to 59 seconds. To have the warning beep indefinitely until it is reset with the Black Resetter key, enter 60 seconds.
Alarm Beep	Enter the number of seconds to sound the alarm beep. The range of valid values is from 1 to 59 seconds. To have the alarm beep indefinitely until it is reset with the Black Resetter key, enter 60 seconds.
Warn w/Horn	Select this option to use the unit's horn for the warning sound instead of the ImpactManager RF beeper.
Alarm w/Horn	Select this option to use the unit's horn for the alarm sound instead of the ImpactManager RF beeper.

4. When finished, click the Save button to save the new Accelerometer profile.

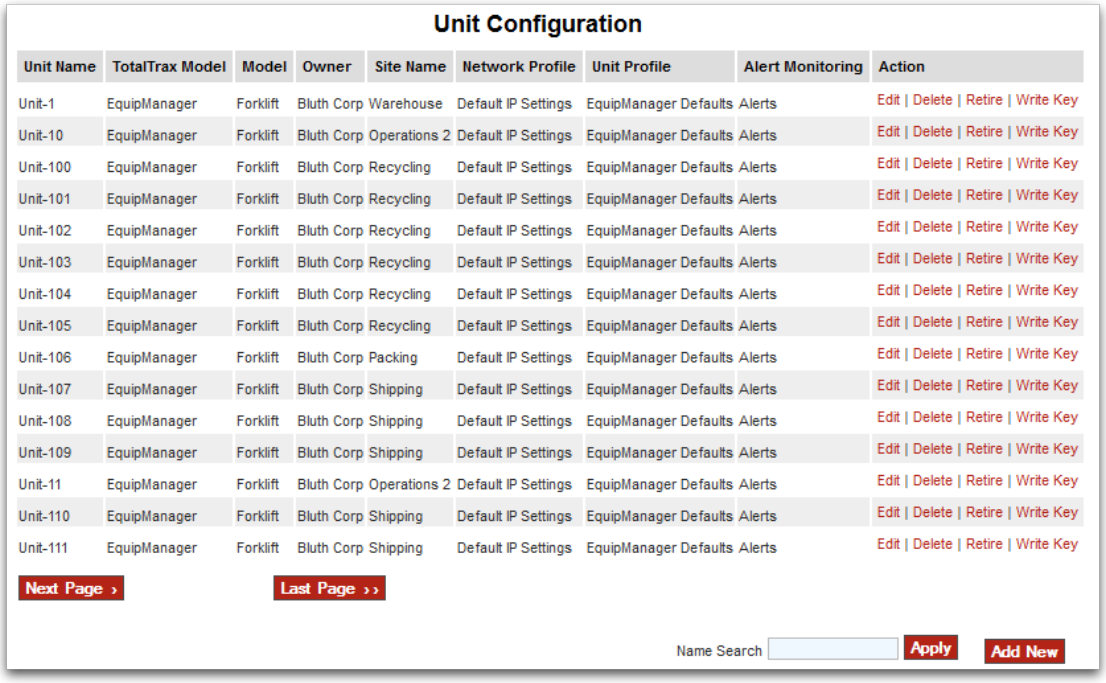
4.3.6 Unit Configuration

Each piece of equipment on which ImpactManager RF is installed must be identified to the software.

To add an entry for each unit:

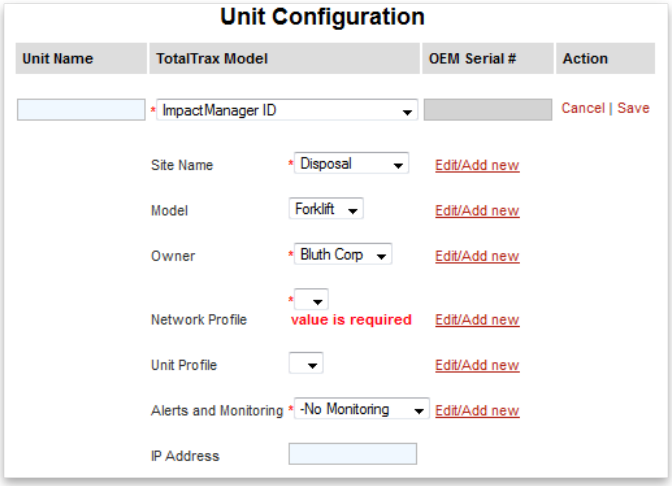
1. If you are not using the Unit Setup Wizard, in the Unit Setup menu, click Unit Configuration.

The Unit Configuration window displays.



2. Click the Add New button.

   The Unit Configuration - Add New window displays



   Refer to the following table for a description of the fields and options.

NOTE: The Edit/Add new links are links to the setup pages for the corresponding field or option.

Unit Configuration Setting	Description
Unit Name	The identity of the unit.
TotalTrax Model	The specific TotalTrax model being used with the unit. Select ImpactManager RF.
OEM Serial #	This field is automatically populated with the serial number of the unit circuit board when data is collected for the first time.
Site Name	The site at which the unit used. For information about setting up sites, refer to "Site Setup" on page 16.
Model	The model of the unit. For information about adding models to the system, refer to "Model and Manufacturer" on page 28.
Owner	The owner of the unit. For information about adding unit owners to the system, refer to "Unit Owners" on page 27.
Network Profile	User-configured settings that allow the unit to communicate across an 802.11 network to the EquipCommand server.
Unit Profile	User configured unit settings.
Alerts and Monitoring	The Alerts and Monitoring option, set up in "Alerts and Monitoring" on page 50.
IP Address	The unit's IP address. If not using DHCP to dynamically assign the unit's IP address, the static IP address entered here will be used for the unit.

3. When finished, click the Save link in the Action column to create the new entry.

Retiring a Unit

Retiring a unit prevents it from being assigned or licensed. However, a retired unit is still included in historical reporting reporting (i.e., in the reporting subsystem, Event History window, and Unit Configuration window).

A unit can be deleted after being retired.

To retire a unit, click the Retire link for the unit entry in the Unit Configuration window. You are prompted to confirm the retire operation. If you confirm the operation, the Retire link changes to an Unretire link.

To unretire a retired unit, click the Unretire link for the unit entry in the Unit Configuration window. You are prompted to confirm the unretire operation.

Deleting a Unit

Deleting a unit removes it from the database. You will not be able to recapture its data or view its data in reports.

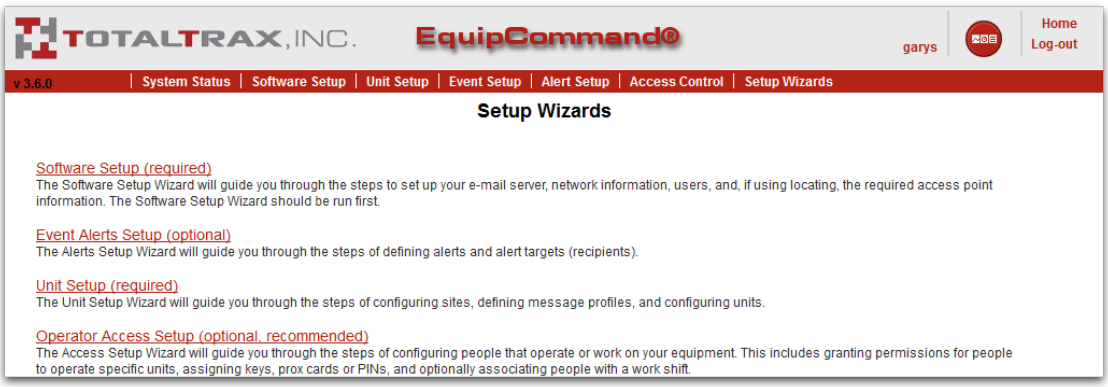
To delete a unit, click the Delete link for the unit entry in the Unit Configuration window. You are prompted to confirm the deletion.

4.4 Operator Access Setup Wizard

The Operator Access Setup Wizard guides you through the steps to give permissions to personnel and assign keys, work shifts, and assignments.

To run the Operator Access Setup Wizard:

1. Click the Access Setup link on the home page.



   The Wizard starts and the first Operator Access Setup window displays.

2. Complete the fields and options in each window, as needed.

   For detailed procedures, refer to the following topics.

3. To advance to the next step within the Wizard, click Next Step.

   To go back a step, click Prev Step.

NOTE: To import operator information from a file, refer to "Operator Import from File" on page 58.

4.4.1 Supervisors

EquipCommand allows you to specify supervisors and the sites where they are located.

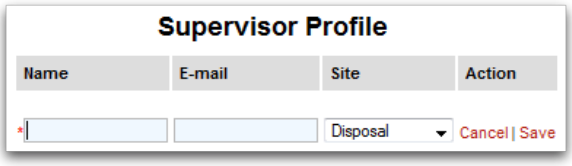
To add a new supervisor:

1. If you are not using the Access Setup Wizard, in the Access Control menu, click Supervisor Profile.

   The Supervisor Profile window displays.

2. Click the Add New button.

   The Supervisor Profile - Add New window displays.



3. Enter the supervisor’s name in the Operator field and select the site from the drop down field.
4. Optionally, enter the supervisor's e-mail address. The supervisor e-mail address can be used to e-mail individual supervisors without the need for setting up alert targets (i.e., supervisors can receive e-mail alerts on impacts).
5. When finished, click the Save link in the Action column to create the new supervisor entry.

4.4.2 Operator and Key Configuration

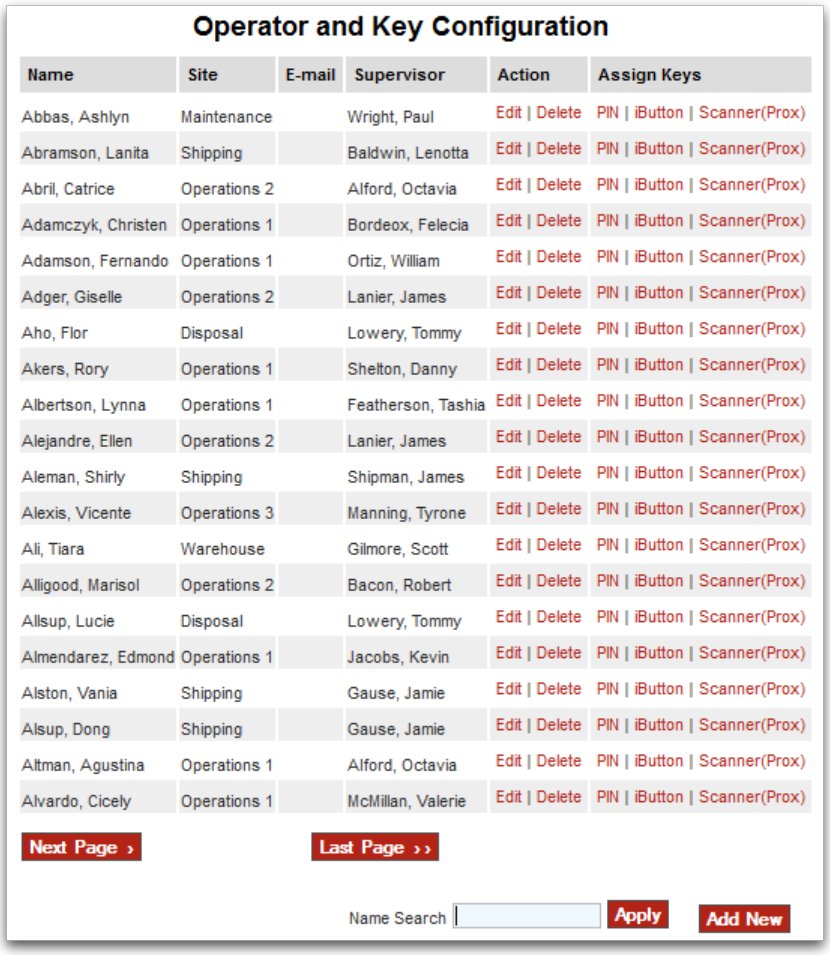
Any person that will interact with ImpactManager RF through the use of an iButton key, proximity card, or infrared barcode card must be identified to the EquipCommand software.

NOTE: The use of PIN codes for keys is not supported by ImpactManager RF.

To add person as an operator:

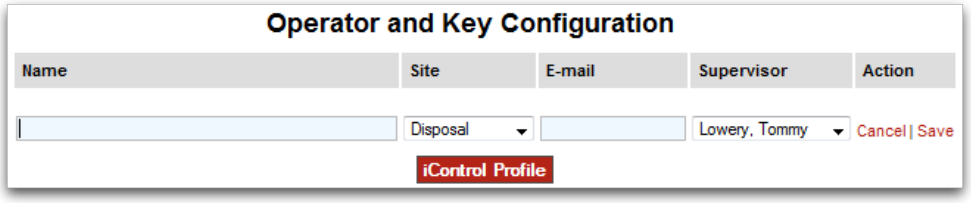
1. If you are not using the Access Setup Wizard, in the Access Control menu, click Operator and Key Configuration.

   The Operator and Key Configuration window displays.



2. Click the Add New button.

   The Operator and Key Configuration - Add New window displays.



3. Enter the operator information, as needed.

   Refer to the table below for a description of the fields and options.

Operator Configuration Fields and Options	Description
Name	Enter the name of the operator (required).
Site	Select the site associated with this operator.
E-mail	Enter the operator's email address.
Supervisor	Select the operator's supervisor.

4. When finished, click the Save link in the Action column to add the operator entry.

After adding an operator, you need to assign a key to the operator. The following key types can be assigned:

- iButton
- Proximity Card and Infrared Barcode Card

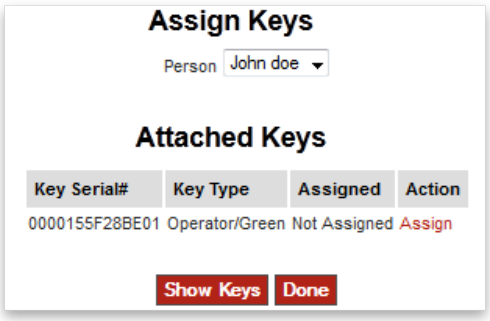
The following topics describe how to assign each of these key types to an operator.

Assigning an iButton Key to an Operator

To assign an iButton key to an operator:

1. Load a Green Operator key into the iButton key reader.
2. In the Operator and Key Configuration window, click the iButton link in the operator entry.

   The Attached Keys window displays.



3. Make sure the correct operator is selected in the Person list.
4. Click the Assign link in the Action column.

   The Green Operator iButton key is assigned to the person.

Assigning a Proximity Card or Infrared Barcode Card Key to an Operator

To assign a proximity card or infrared barcode card key to an operator:

1. In the Operator and Key Configuration window, click the Scanner (Prox) link in the operator entry.

   The Assign Prox Cards window displays.

2. Complete the fields and options in the window.

   Refer to the table below for a description of the fields and options.

Assign Prox Cards Fields and Options	Description
Person	The person to whom you want to assign the key.
Key Type	The key type you want to assign.
Scanner Device Type	The type of scanner device you are using.
Scanner on Port	The port to which the scanner is connected.

3. When finished, click the Click Here and Scan button to assign the card.

You have about 15 seconds to scan the card. If you do not scan the card in time, a message displays in the window indicating that nothing was scanned. If you do scan the card in time and it is properly assigned, a message displays in the window indicating that the card was successfully assigned and to what operator it was assigned.

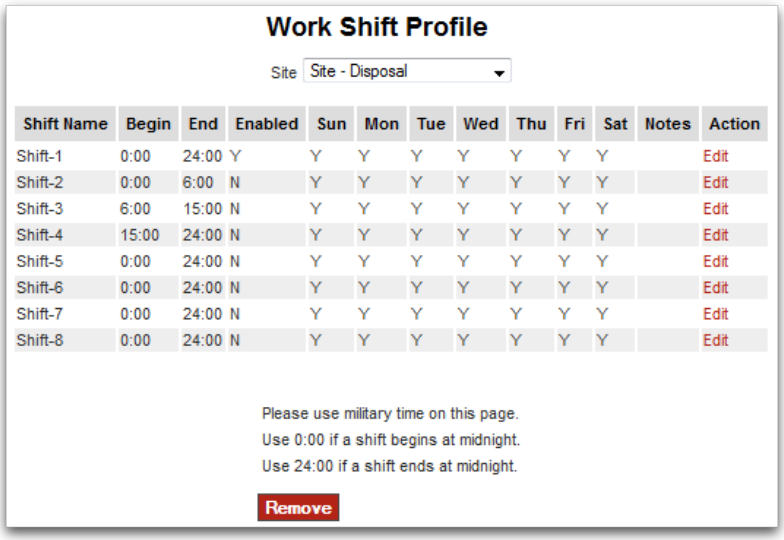
4.4.3 Work Shift Profiles

You can configure up to eight work shifts. Work shifts are defined as predetermined periods of time that specific employees work.

To define the work shifts:

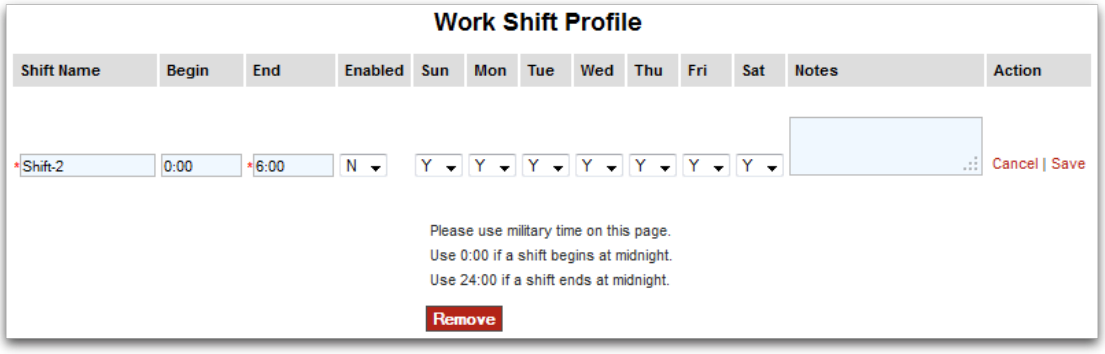
1. If you are not using the Access Setup Wizard, in the Access Control menu, clicks Work Shift Profile.

   The Work Shift Profile window displays.



2. Click the Edit link for the shift that you want to define.

   The Work Shift Profile - Edit window displays.



3. Complete the fields and options in the window.

Refer to the table below for a description of the fields and options.

Work Shift Profile Fields and Options	Description
Shift Name	Enter the name of the shift.
Begin	Enter the shift start time.
End	Enter the shift end time
Enabled	Select Y (for Yes) to enable this shift.
Sun through Sat	Select Y (for Yes) in the box of the days to which this shift applies.
Notes	Add notes for the shift, if needed.

4. When finished, click the Save link to define the shift.

NOTE: Repeat this procedure for each shift that needs to be defined.

4.4.4 Operator Assignments

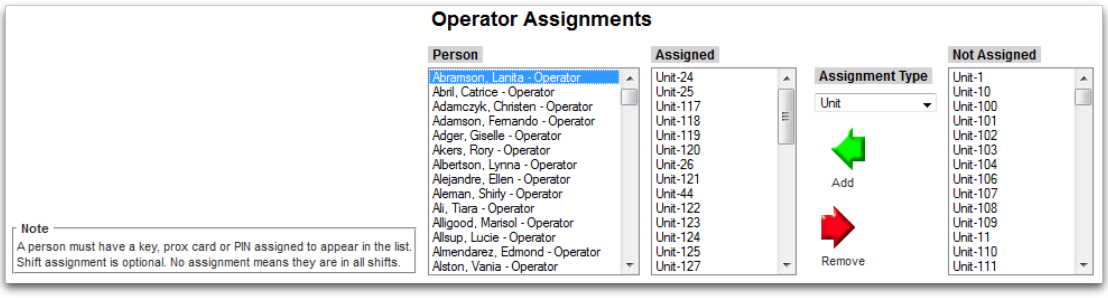
In Key Rules settings of the Unit Profile Setup window (refer to "Unit Profiles" on page 29), a choice was made as to whether all iButton keys would be accepted or if specific keys were to be limited to specific units. If controlling which keys are used with specific units, all operators must be assigned to a unit, a model (as defined in "Setting Up Equipment Groups" on page 56), and/or a work shift (as defined in "Work Shift Profiles" on page 45).

To make personnel assignments:

1. If you are not using the Access Setup Wizard, in the Access Control menu, click Operator Assignments.

   The Operator Assignments window displays.

   An operator can be assigned to a unit, a model, or a shift.



2. To change assignments, select the operator in the Person list.

Operators will not appear in the Person list unless they have been assigned a key card or PIN.

3. Select what you are assigning to the operator in the Assignment Type list.
4. To add an assignment, select entries in the Not Assigned list and then click the Add arrow button.

   To remove an assignment, select entries in the Assigned list, select the appropriate entry in the Assignment Type list, and then click the Remove arrow button.

4.4.5 Operator Certifications

The equipment certifications for each operator can be entered and tracked.

The EquipCommand software monitors the certification of each operator. By default, when an operator is within 30 days of their certification expiring, a Certification Expiring event is generated. The Administrator can adjust the 30-day advance notice to the number of days that are appropriate or required.

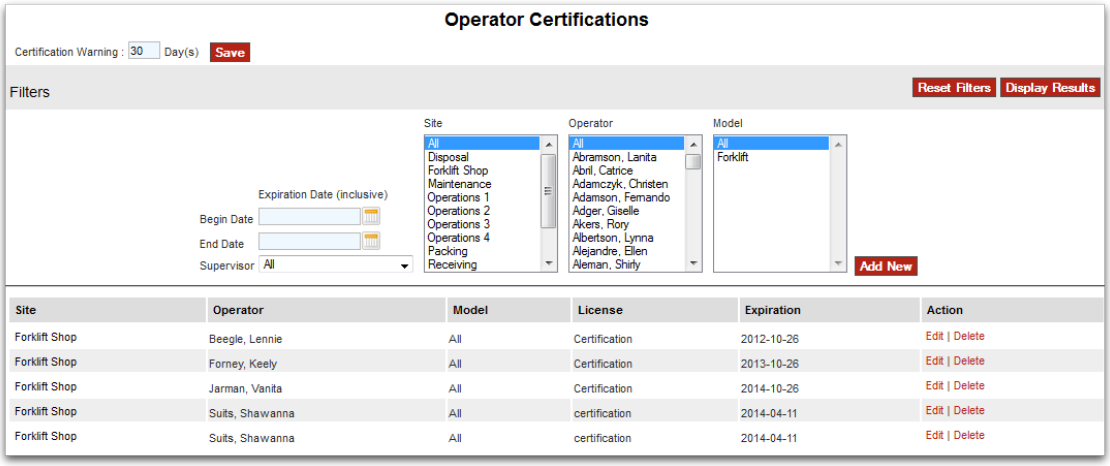
Certifications can be used to limit equipment operation specifically to operators with the proper certification. To enable this functionality, The Enforce Operator Certifications check box option in the Site Profile window must be selected (refer to "Site Setup" on page 16).

NOTE: The restriction of operation by certification will be enforced only if the administrator has chosen to use dedicated operator lists, as described in "Operator Assignments" on page 46.

To enter and track equipment certifications for an operator:

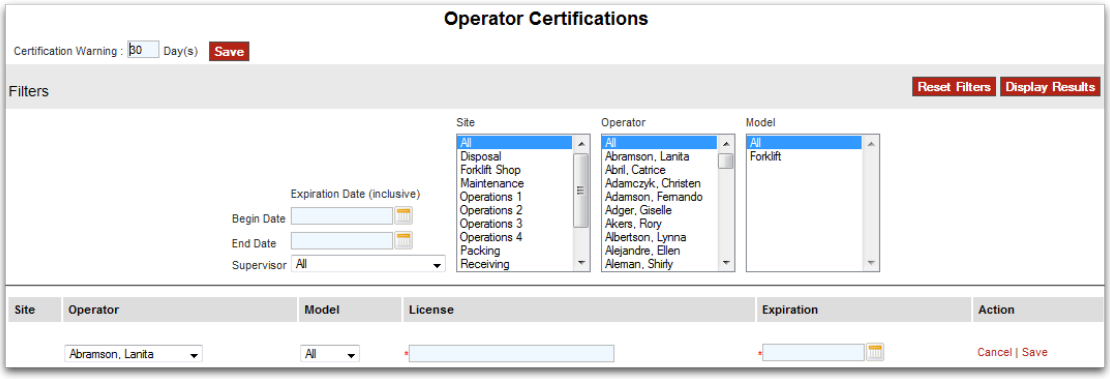
1. If you are not using the Access Setup Wizard, in the Access Control menu, click Operator Certificates.

   The Operator Certifications window displays.



2. Click the Add New button.

   The Operator Certifications - Add New window displays.



3. Complete the fields and options in the window.

   Refer to the table below for a description of the fields and options.

Operator Certifications Fields and Options	Description
Operator	Select the operator name.
Model	Select the model that applies to the certification.
License	Enter the license number.
Expiration	Enter the certification expiration date.

4. When finished, click the Save link in the Action column to save the operator certification entry.

Filtering the List of Operator Certifications When Editing

To filter the list of operator certifications when editing existing certifications:

1. Enter the filter criteria in the fields and lists at the top of the Operator Certifications window.

   You can filter by any combination of the following:

   - Date range for the expiration date
   - Operators' supervisor
   - Site
   - Operator
   - Unit model

2. After entering the filter criteria, click the Display Results button.

Only those operator certification entries that match the filter criteria are displayed.

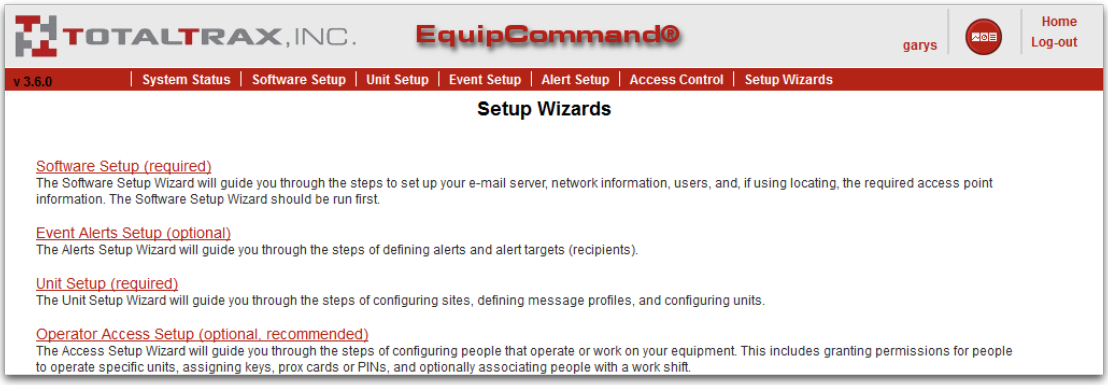
To clear the entered filter criteria, click the Reset Filters button.

4.5 Event Alerts Setup Wizard

The Event Alerts Setup Wizard guides you through the steps to define alerts and enable and configure instant alerts and threshold warnings.

To run the Event Alerts Setup Wizard:

1. Click the Event Alerts Setup link on the home page.



The Wizard starts and the first Event Alerts Setup window displays.

2. Complete the fields and options in each window, as needed.

   For detailed procedures, refer to the following topics.

3. To advance to the next step within the Wizard, click Next Step.

   To go back a step, click Prev Step.

4.5.1 Alert Targets

The EquipCommand software can notify specific individuals via e-mail when an event occurs. The contact information for the individuals to be notified must be entered in the Alert Targets screen.

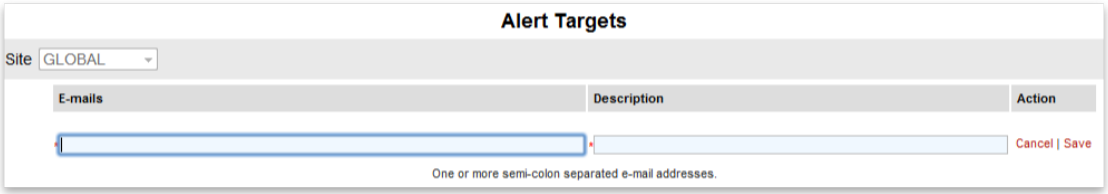
To set up an Alert Target:

1. If you are not using the Event Alerts Setup Wizard, in the Alert Setup menu, click Alert Targets.

   The Alert Targets window displays.

2. To add an Alert Target, click the Add New button.

   The Alert Targets - Add New window displays.



3. Enter the e-mail address of the contact in the Email field. You can enter multiple e-mail addresses by separating them with a semi-colon.
4. Enter a description of the contact in the Description field.
5. When finished, click the Save link in the Action column to add the new contact as an Alert Target.

To test an Alert Target, click its Test link. An e-mail is sent to the e-mail addresses assigned to the target.

To delete an Alert Target entry, click its Delete link.

4.5.2 Alerts and Monitoring

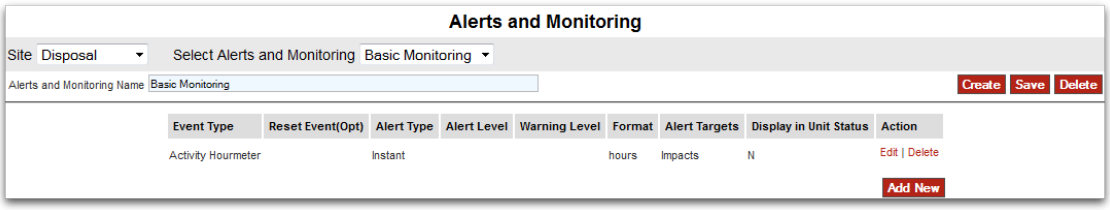
A number of standard events represent the accumulation of a quantity of time or counts, as defined in the Alerts and Monitoring Setup wizard. The EquipCommand software enables these types of events to be interactively viewed and monitored.

The Alerts and Monitoring window allows you to select events and then set parameters regarding actions related to them. Any listing added to this window appears in the Unit Status window, as described in "Unit Status" on page 77, if Yes is selected for the Display in Unit Status option when adding a new Alert listing.

Opening the Alerts and Monitoring Window

If you are not using the Event Alerts Setup Wizard, in the Alert Setup menu, click Alerts and Monitoring.

The Alerts and Monitoring window displays.



Changing the Alert Type

To change the type of Alerts that are listed, choose the profile from the Select Alerts and Monitoring list.

Creating an Alert Profile

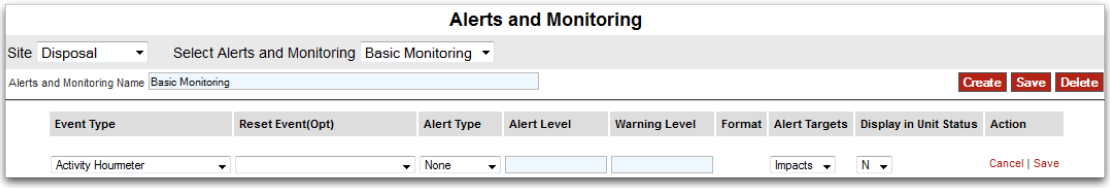
To create a new profile, click the Create button, enter the name of the new profile you want to create, and click the Save button.

Adding an Event

To add an event to be monitored:

1. Click the Add New button.

   The Alerts and Monitoring - Add New window displays.



2. Complete the fields and options in the window.

   Refer to the table below for a description of the fields and options.

Event Fields and Options	Description
Event Type	Select the appropriate event type.
Reset Event(Opt)	Select the appropriate Reset event, if needed. The Reset event is used to reset any related timers or counters. There are a number of standard Reset events. Verify that you are selecting the appropriate Reset event. A new event representing the correct Reset event might need to be created as described in "Creating Custom Events" on page 54.
Alert Type	Possible settings are: • Instant: E-mail is generated immediately upon receipt of the event. • Conditional: E-mail is only sent after the Alert level threshold has been met.
Alert Level	Enter the timer or counter level that would be considered an Alert level, indicating the count or time when, if surpassed, an e-mail message would be generated, alerting someone to the level or count.
Warning Level	A timer or counter level of a lesser amount than the Alert level. This serves as notice to personnel that the event is nearing the Alert level threshold.
Format	The unit of measure that is defined in the event configuration. For more information, refer to "Event Configuration" on page 53.
Alert Targets	Select the Alert targets to which the alert should be sent.
Display in Unit Status	Select whether this event will be displayed on the Unit Status window.

3. When finished, click the Save link in the Action column to add the event.

NOTE: Alert targets and the corresponding e-mail addresses must be pre-configured as described in "Alert Targets" on page 49.

Example Event

Suppose a Run Time event was created, mapped to a standard event, and configured so that when the 100 hours is reached, the Run Time event will be generated.

If this Run Time event is added to the list in the Alerts and Monitoring window, it will be included in the Unit Status window when it occurs, showing the reported time and calculated status.

4.6 Custom Events

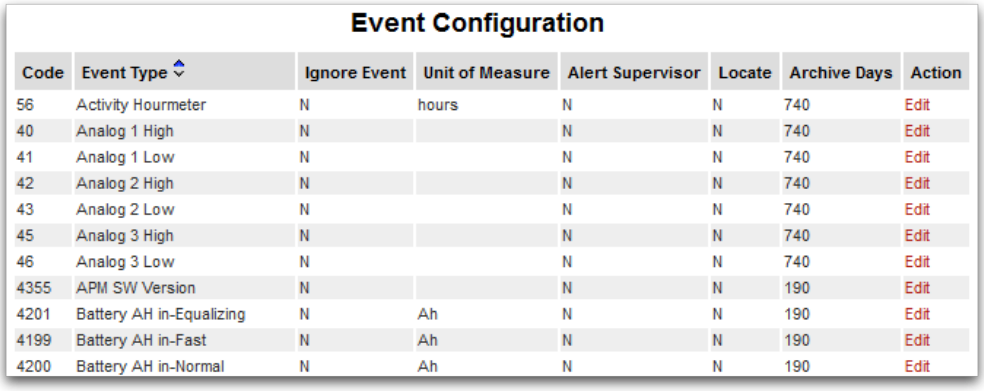
The Event Setup menu options allow you to define event categories. These menu options are described in the following topics.

4.6.1 Event Configuration

The EquipCommand software provides 42 pre-defined events. Events are markers that provide a mechanism to time- and date-stamp particular actions or results. These events are generated by the unit and sent to the software (through use of the Yellow Manager's Key) so that the user can review them. For a description of these pre-defined event types, refer to "Pre-Defined Event Types" on page 79.

To view these event types, in the Event Setup menu, click Event Configuration.

The Event Configuration window displays.



Event Configuration

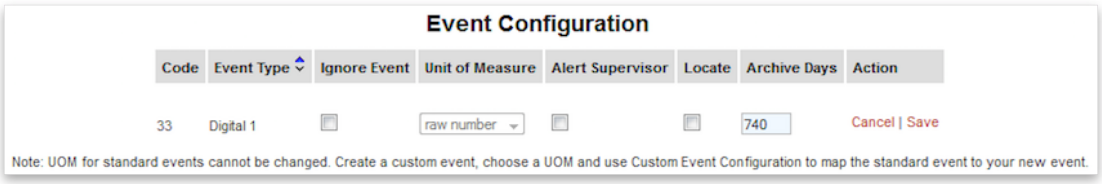
Code	Event Type	Ignore Event	Unit of Measure	Alert Supervisor	Locate	Archive Days	Action
56	Activity Hourmeter	N	hours	N	N	740	Edit
40	Analog 1 High	N		N	N	740	Edit
41	Analog 1 Low	N		N	N	740	Edit
42	Analog 2 High	N		N	N	740	Edit
43	Analog 2 Low	N		N	N	740	Edit
45	Analog 3 High	N		N	N	740	Edit
46	Analog 3 Low	N		N	N	740	Edit
4355	APM SW Version	N		N	N	190	Edit
4201	Battery AH in-Equalizing	N	Ah	N	N	190	Edit
4199	Battery AH in-Fast	N	Ah	N	N	190	Edit
4200	Battery AH in-Normal	N	Ah	N	N	190	Edit

Editing a Pre-Defined Event

To edit the settings for a pre-defined event:

1. Click the event's Edit link.

   The Event Configuration - Edit window displays.



Event Configuration

Code	Event Type	Ignore Event	Unit of Measure	Alert Supervisor	Locate	Archive Days	Action
33	Digital 1	☐	raw number	☐	☐	740	Cancel | Save

Note: UOM for standard events cannot be changed. Create a custom event, choose a UOM and use Custom Event Configuration to map the standard event to your new event.

2. Modify the event settings, as needed.

   Refer to the table below for a description of the settings.

Pre-Defined Event Settings	Description
Ignore Event	Select this option to have the system ignore this event. The event will not be logged.
Unit of Measure	Select the units for the event.
Alert Supervisor	If this option is selected, an e-mail will be sent automatically to an operator's supervisor upon generation of that specific event.
Locate	Select this check box to enable event-generated locating. **NOTE:** Because ImpactManager RF does not allow event-generated locating, leave this check box cleared.
Archive Days	Enter the number of days for which this type of event will be archived. After this time period, the event will be automatically purged from the database. The default amount of 740 days is typically used.

3. When finished, click the Save link in the Action column to save the setting changes.

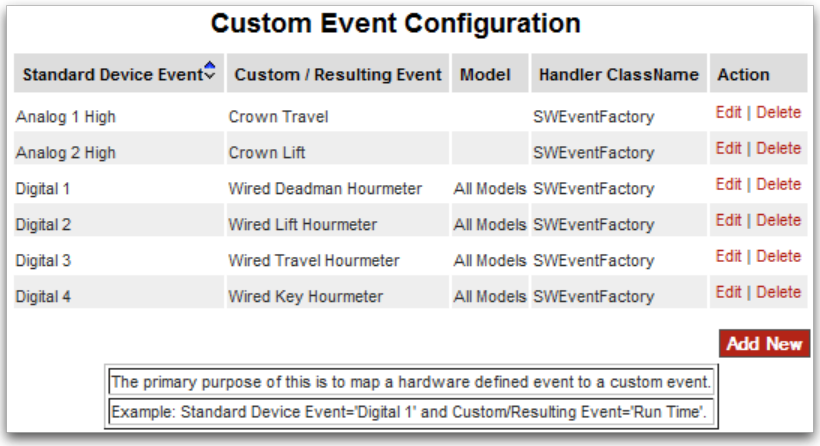
4.6.2 Creating Custom Events

The EquipCommand software allows an Administrator to create new events that might better compliment their environment and application. A simple example involves the default Hit event that signifies when the ImpactManager RF Impact sensor has been triggered. For some environments, the word **Hit** might not be correct. In this instance, the Administrator might consider creating a new event called Impact Sensor Trigger.

To create a new event:

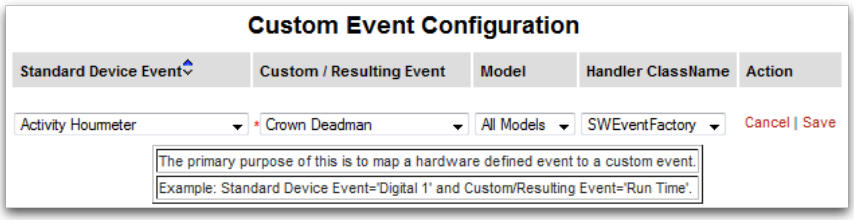
1. In the Event Setup menu, click Custom Event Configuration.

   The Custom Event Configuration window displays.



2. Click the Add New button.

   The Custom Event Configuration - Add New window displays.



3. Enter the event information.

   Refer to the following table for a description of the fields and options.

Custom Event Fields and Options	Description
Standard Device Event	Select the standard device event on which the custom event will be based.
Custom/Resulting Event	The name for the event.
Model	Select to which model the event corresponds.
Handler Class Name	The only choice is SWEventFactory. An internal system setting.

4. When finished defining the new event, click the Save link in the Action column to save the event.

4.7 Additional Information Setup Not Covered in the Wizards

While the Setup Wizards take you through the basics of setting up the EquipCommand software, there is additional information that needs to be set up.

Setting up this information is covered in the following topics.

4.7.1 Changing Passwords and the Time Zone

An EquipCommand administrator can change user passwords and set the time zone to be used in the EquipCommand interface.

Changing Your Password

Access to the EquipCommand software is provided through the use of a username and password. Any level user can change their own password.

To change a password:

1. In the Software Setup menu, click Change Password.

The Change Password/Time Zone window displays.

2. In the Old Password field, enter your old (current) password.
3. In the New Password field, enter the new password you want to use.
4. In the Confirm Password field, re-enter your new password.
5. When finished, click the Change Password button.

Setting the Time Zone

Open the Change Password/Time Zone window as described above and select the time zone from the list.

4.7.2 Setting Up Equipment Groups

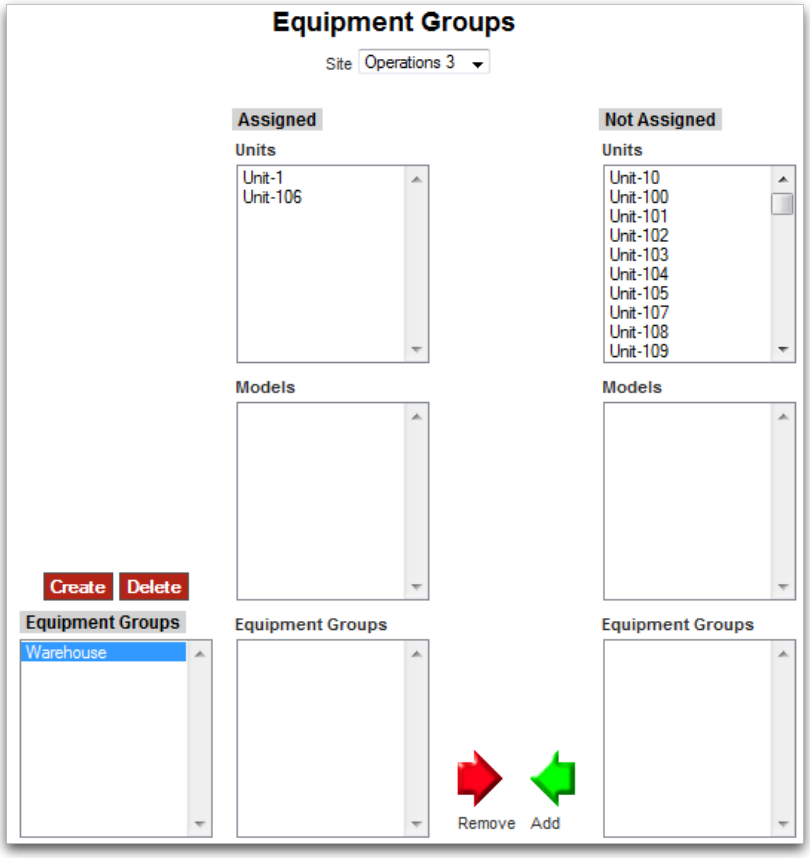
Equipment Groups allow trucks of disparate makes/models to be grouped so that operators can be assigned to a group.

For example, the shipping department might have many different types of forklifts. However, all shipping personnel must have the ability to drive this equipment. Rather than having to assign each unit to every shipping employee, each unit would be assigned to the Shipping Group. This would allow each shipping employee to be assigned to the single Shipping Group.

To set up an Equipment Group:

1. In the Access Control menu, click Group Assignments.

   The Equipment Groups window displays.



2. To create a new group, click the Create button, name your group (e.g., Shipping), and then click Save.

   - OR -

   Select an existing group to modify it.

3. In the Not Assigned column, select one or more units, models, or existing equipment groups to be assigned to the new group.

4. Click the Add arrow button.

   The selected vehicles move to the Assigned column to show they are now assigned to the group.

   The Equipment Group will now be included in the Assigned or Not Assigned lists in the Operator Assignments window, along with individual unit names. For more information about assigning an operator to individual units or to an Equipment Group, refer to "Operator Assignments" on page 46.

4.7.3 Operator Import from File

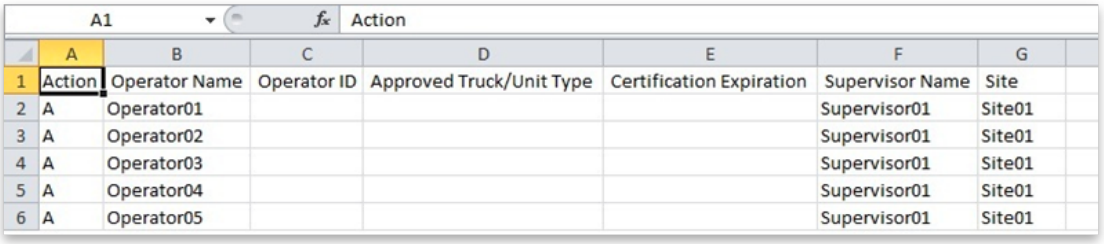
EquipCommand allows you to upload operator names, badge numbers (internal), and certifications from a file. This greatly decreases the effort for adding operator information into the system.

The file must meet the following specifications:

- Files to be uploaded must be in a comma-delimited format that is saved as either plain text or exported from a spreadsheet application (for example, Excel) in a .csv format.
- Each operator record must be entered on a separate line. The first line in the file is ignored and can be used to include a description (for example, First Shift).
- Fields should be separated by a comma. Empty fields should be denoted by either entering a space followed by a comma or by entering a single comma.
- Record fields must consist of the following and in the given order: Operator Name, Operator ID, Approved Truck/Unit Type, Certification Expiration, Supervisor Name. Refer to the table below for a description of each field.

Import File Record Fields	Description
Operator Name	The name as it will appear in EquipCommand. Multiple records can exist for the same operator to accommodate multiple "approved truck/units", "certification expirations", or "supervisors". Each new record for the operator must be entered on a separate line in the file.
Operator ID	A valid scanner/proximity card number.
Approved Truck/Unit type	Should be a valid truck/unit type as already entered into EquipCommand.
Certification Expiration	Should be in the yyyymmdd date format.
Supervisor Name	Should be a valid supervisor name already entered into EquipCommand

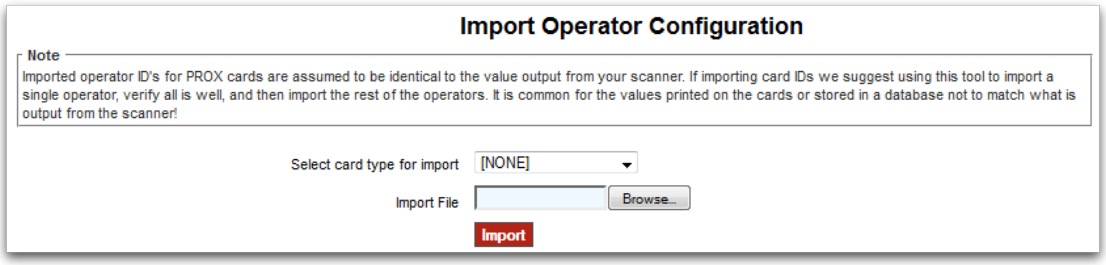
The following figure shows an example of the spreadsheet layout for an operator import CSV file.



To import operator information from a file:

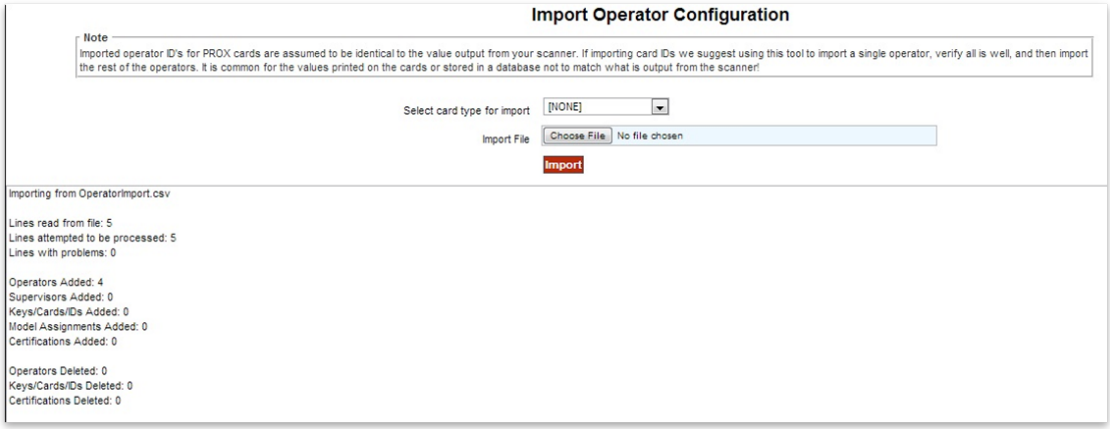
1. In the Access Control menu, click Import Operator Configuration.

   The Import Operator Configuration window displays.



2. Select the key card type to be used by the operators whose configuration records are being imported.
3. Click the Browse button and choose the file to be imported.
4. Click the Import button.

   The status of the import operation is displayed in the window.



NOTE: If there are import problems, contact TotalTrax Technical Support for assistance.

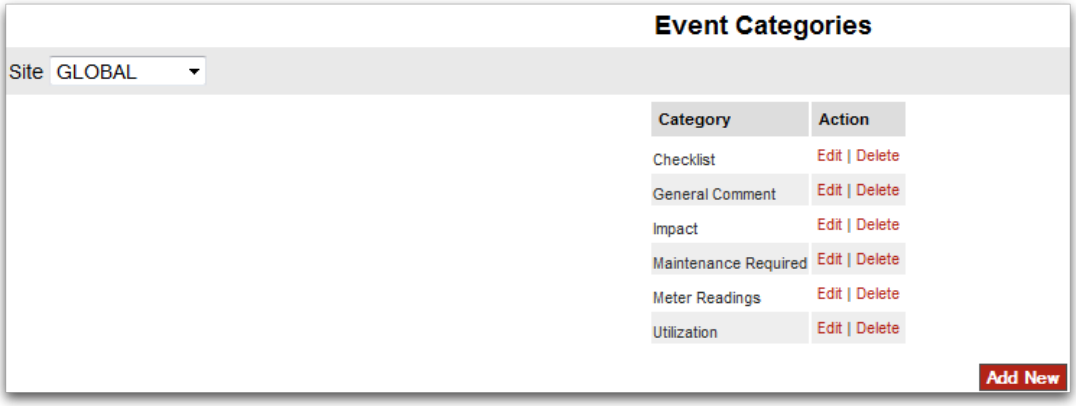
4.7.4 Setting Up Event Categories

The EquipCommand software allows the Administrator to create categories for all events. This categorization provides significance or notation to all events. Examples include Injury, Damage, and Damage + Injury.

To add an event category:

1. In the Event Setup menu, click Event Categories.

   The Events Categories window displays.



2. Click the Add New button.
3. In the field that displays, enter the category name and then click the Save link.

Section 5. Using Keys

The primary interface between the EquipCommand software and the ImpactManager RF unit are the keys. Keys can be iButtons, proximity cards, and infrared barcode cards. This section describes each of the key types and how they are used.

The primary non-RF interface between the EquipCommand software and the ImpactManager RF unit are keys. Keys can be iButtons, proximity cards, and infrared barcode cards. This section describes each of the key types and how they are used.

5.1 Accessing Units with the Green Operator Key

The Green Operator key is used to allow operator access to a unit.

5.2 Performing a Safety Check with the Green Operator Key

The Green Operator key can be used to provide a Safety Check event. This Safety Check event can be generated on an "as needed" or "as required" basis.

To generate a Safety Check event, insert and hold the Green Operators key in the ImpactManager RF User Interface Port for five seconds.

When the key is first inserted, ImpactManager RF chirps once, generating an operator log on.

At the end of the five seconds, ImpactManager RF chirps once, warbles, and then chirps once again, confirming that the Safety Check event has been generated. A Safety Check event is added to the Event History database.

5.3 Loading Unit Settings Using Keys

You use the Yellow Manager key and Red Settings key to load a unit's configuration information and operator list into the unit. If a secure wireless network is being used, you use the Orange Certificate key to load the required wireless certificates into the unit. For information about using these keys to configure a unit, refer to "Section 6. Loading Unit Configuration Information".

5.4 Manually Retrieving Events Data from a Unit

To manually retrieve events data from a unit:

1. Clear the data on the Yellow Managers key. Refer to "Show Attached Keys " on page 64 and "Clearing Data from an Attached Yellow Managers or Red Settings Key" on page 64.
2. Insert the Yellow Managers key into the unit's ImpactManager RF User Interface Port.

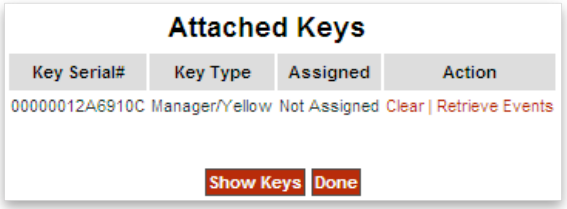
   When data retrieval is complete, ImpactManager RF will chirp two times.

NOTE: Do not remove the Yellow Managers key until you hear the two chirps. The data transfer can take 15 to 30 seconds.

NOTE: Multiple units can be downloaded into one Yellow Manager key depending on the number of events in the units.

3. Take the Yellow Managers key to the computer running the EquipCommand software, and insert the key into the iButton key reader.
4. To retrieve the data from the key, in the Access Control menu, click Attached Keys.

   The Attached Keys window displays.



5. Click the Retrieve Events link of the key entry for the Yellow Managers key whose events data you want to retrieve.

   A message displays when the retrieval process is complete, indicating the success or failure of the date retrieval operation.

To clear event data, click the Clear link of the key entry for the Yellow Managers key whose events data you want to clear.

To poll the key reader for any key that has been plugged into the reader after the Write Settings Keys window has loaded, click the Show Keys button.

When you are finished retrieving the data from the key, click the Done button.

5.5 Performing Inspections and Lockouts with the Blue Maintenance Key

The Blue Maintenance key performs the following functions:

- Provides an Inspection event
- Provides a Lockout of the unit so that operating access is denied
- Resets the Maintenance timer after it has expired

To record an inspection event, touch the Blue key to the ImpactManager RF User Interface Port. ImpactManager RF chirps once to confirm the action and an Inspection event is recorded.

To lockout the equipment, insert and hold the Blue key in the User Interface Port for three seconds. The User Interface Port LED flashes at 1-second intervals. The unit is now disabled and a Lockout event is recorded.

To release the equipment from lockout, touch a Blue key to the User Interface Port. ImpactManager RF chirps once to confirm the release and a Lockout event is recorded.

5.6 Resetting ImpactManager RF with the Black Resetter Key

The Black Resetter key resets an ImpactManager RF that has been set up to sound an alarm and/or shutdown the unit when an impact occurs. The Black Resetter key does not collect data.

To use the Black Resetter key, touch it to the user interface port while ImpactManager RF is alarming and/or has shut the lift down.

The alarm turns off and the unit is released for operation. A Reset Shut Down Mode event is added to the Event History database.

5.7 Key Tools

The primary non-RF interface between the EquipCommand software and the ImpactManager RF unit are the keys. The Access Control menu in the menu bar provides various utilities related to key use.

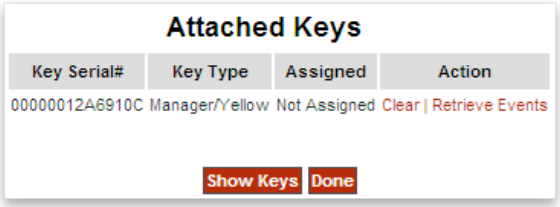
5.7.1 Show Attached Keys

The Show Attached Keys window allows you to scan an iButton to determine the type of key being read and the serial number of the key being scanned.

To scan a key:

1. Insert the key into the key reader.
2. In the Access Control menu, click Attached Keys.

   The Attached Keys window displays, listing the key's serial number, key type, who the key has been assigned to, and links for the available actions.



If you insert another key with the Attached Keys window displayed, click the Show Keys button to recognize the newly inserted key.

Retrieving Event Data from an Attached Yellow Managers Key

You can retrieve unit event data from a Yellow Managers key.

To retrieve the unit event data from the key in the key reader to the EquipCommand server, click the key entry's Retrieve Events link.

Clearing Data from an Attached Yellow Managers or Red Settings Key

You can clear the data from a Yellow Managers key or Red Settings key.

To clear the data on the attached key, click the key entry's Clear link.

5.7.2 Assigned Keys

The Assigned Keys window lists all keys that have been assigned to individuals.

To show all assigned keys, in the Access Control menu, click Assigned Keys.

The Assigned Keys window displays.

Each operator, along with the serial number and type of key they have been assigned, is displayed. Any operator entry in the list can be:

- **Blocked (disabled).** Click the entry's Block link. That operator's key is added to the Blocked Key list, which can viewed on the Blocked Keys window. You can also block additional keys from that window. Refer to "Blocked Keys" on page 66.

NOTE: When blocking a key from the Assign Keys window, the note for the key in the Blocked Key list is populated with the user who performed the block and the date. So you might want to go to the Blocked Keys window and edit the note to explain why the block was done, the case number if your organization tracks why the key was blocked, the date the key is to be released, or any other information that is needed.

- **Deleted.** Click the entry's Delete link. The key and its related assignments are removed from the database.

To sort the listing by Name, Key Serial, or Key Type, click the appropriate column heading.

5.7.3 Blocked Keys

The EquipCommand software allows you to block specific keys from being used. You must identify the key serial number to block it.

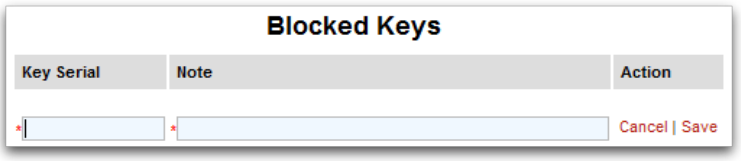
To block a key or see what keys are already blocked:

1. In the Access Control menu, click Blocked Keys.

   The Blocked Keys window displays.

2. To add a blocked key, click the Add New button.

   The Blocked Keys - Add New window displays.



3. Enter the key serial number.
4. A description of the key being blocked must be entered in the Note field.

   The entry can indicate who blocked the key and the date/time of the block, explain why the block was done, include the case number if your organization tracks why the key was blocked, include the date the key is to be released, or any other information that is needed.
5. When finished, click the Save link in the Action column to add the key to the Blocked Keys list.

NOTE: Even if a key is added to the Blocked Keys list, the ImpactManager RF unit will continue to accept the key until a new Operators List is loaded into the unit. For information about loading an Operators List into a unit, refer to "Loading the Operators List onto the Yellow Managers Key" on page 71 and "Loading the Unit Settings from Keys into the Unit" on page 73, or to "Loading Unit Configurations over the Wireless Network" on page 74.

Section 6. Loading Unit Configuration Information

Once the unit configuration information has been setup, as covered in "Section 4. System Configuration", the units can be loaded with their configuration and operators list. The topics in this section explain how to load this information into a Red Settings key, Yellow Managers key, and Orange Certificated key, and then upload the information from these keys into ImpactManager RF on the unit.

The initial loading of a unit's configuration information must be performed using keys. Subsequent updates to the configuration information can be performed wirelessly; for more information about using the wireless method, refer to "Loading Unit Configurations over the Wireless Network" on page 74.

6.1 Loading Unit Configuration Information onto the Red Settings Key

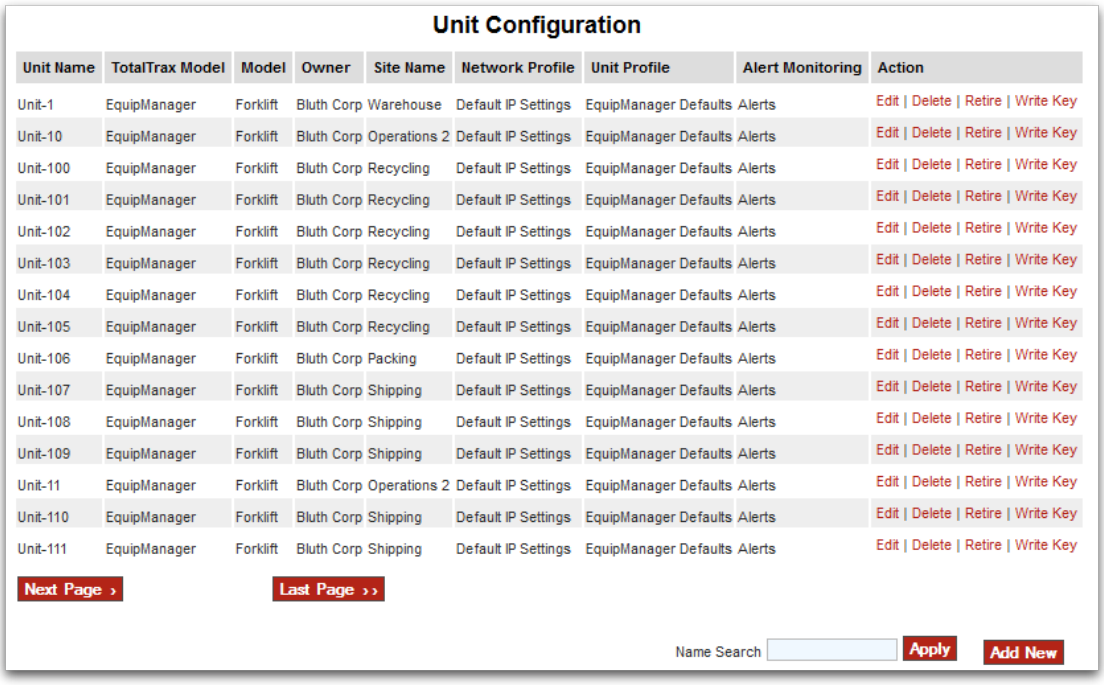
Before loading the unit's configuration information onto the Red Settings key, make sure the following features are enabled for the unit in its Unit Profile (refer to "Unit Profiles" on page 29):

- Upload to Manager Key: If this option is not selected, you cannot download information with a Yellow Manager’s key.
- Clear after Manager Key Upload: If this option is not selected, the unit could fill up its memory (memory can store up to 500 events).

To load a unit's configuration onto a Red Settings key:

1. Insert a Red Settings key into the iButton key reader.
2. In the Unit Setup menu, click Unit Configuration.

   The Unit Configuration window displays.



3. Click the Write Key link for the unit whose configuration information is being loaded onto the key.

NOTE: Make sure that you click the Write Key link for the correct unit.

The Write Settings window displays and the writing process begins.

A message displays when the writing process is complete and the key is successfully loaded with the unit's configuration information.

To poll the key reader for any key that has been plugged into the reader after the page has loaded, click the Show Keys button.

6.2 Loading the Operators List onto the Yellow Managers Key

The next step in implementing ImpactManager RF on the unit is to load the list of approved operators onto a Yellow Managers Key.

NOTE: The Allow All Operator Keys in the unit's Unit Profile must be cleared for the drivers list to be used by the unit. Refer to "Unit Profiles" on page 29.

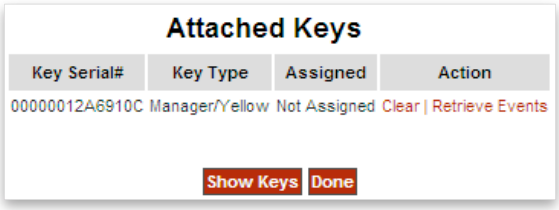
Clearing the Yellow Managers Key

The Yellow Managers key must first be cleared before loading a new operators list.

To clear a Yellow Managers key:

1. Insert the key into the key reader.
2. In the Access Control menu, click Attached Keys.

   The Attached Keys window displays.



3. Click the key's Clear link.

Transferring the Operators List to the Yellow Managers Key

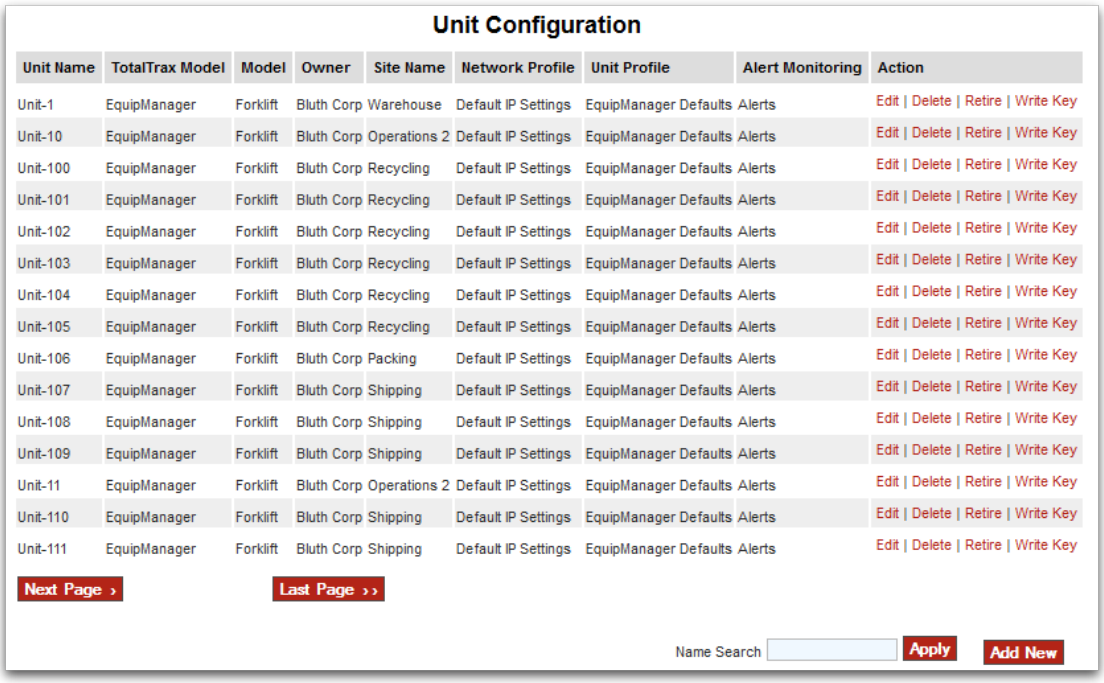
To transfer the Operators List to the cleared Yellow Managers Key:

1. Make sure that the Yellow Managers key is inserted in the reader.

NOTE: The Yellow Manager Key must be in the reader when the write process begins.

2. In the Unit Setup menu, click Unit Configuration.

   The Unit Configuration window displays.



3. Click the Write Key link for the unit whose operator list is being loaded onto the key.

NOTE: Make sure that you click the Write Key link for the correct unit.

The Write Settings window for that unit displays.

4. Click the Secondary link.

   The list of operators is written to the Yellow Managers key.

   A message displays when the writing process is complete, indicating the success or failure of the transfer operation.

To poll the key reader for any key that has been plugged into the reader after the Write Settings Keys window has loaded, click the Show Keys button.

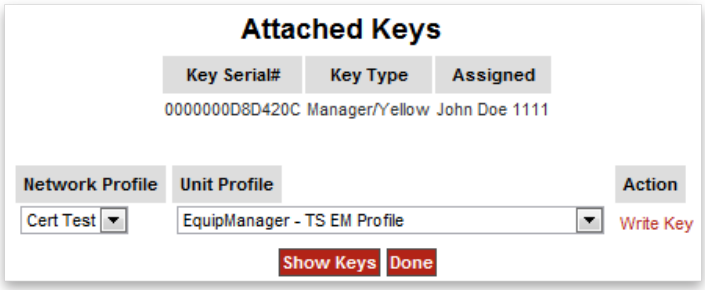
When you are finished transferring the operator list for the unit, click the Done button.

6.3 Loading the Unit Wireless Certificates onto the Orange Certificate Key

To load a unit's wireless certificates onto the Orange Certificate key:

1. Insert the Orange Certificate key into the iButton key reader.
2. In the Unit Setup menu, click Write Key with Certificate Files.

   The Attached Keys window for wireless certification files displays.



3. In the Network Profile list, select the unit's network profile.
4. In the Unit Profile list, select the unit's profile.
5. Click the Write Key link in the Action column.

   The certificate files for the unit are written to the key.

6.4 Loading the Unit Settings from Keys into the Unit

After loading the unit configuration information onto a Red Settings key, the unit's operator list onto a Yellow Managers key, and the unit's wireless certificates onto an Orange key, you are ready to load the unit's settings into the unit.

To load the unit's settings into the unit, perform the following steps in the sequence shown:

1. Insert the Red Settings key into the unit's ImpactManager RF User Interface Port.

   When the data transfer is complete, ImpactManager RF sounds three chirps.

NOTE: Do not remove the key until you hear the chirps. The data transfer can take 15 to 30 seconds.

2. Remove the Red Settings key and insert the Yellow Managers key into the unit's ImpactManager RF User Interface Port.

   When the Operators List has finished loading, ImpactManager RF sounds two sets of two chirps.

3. Remove the Yellow Managers key and insert the Orange Certificate key into the unit's ImpactManager RF User Interface Port.

   When the wireless certificates have finished loading, ImpactManager RF sounds a chirp and then after a minute sounds another chirp.

The unit should now be configured.

Once authenticated, the unit will begin communicating with the EquipCommand software.

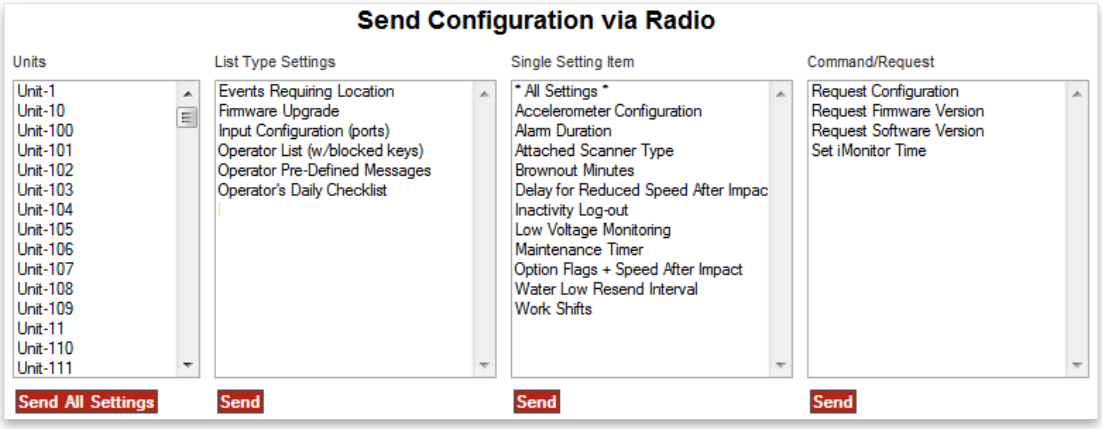
6.5 Loading Unit Configurations over the Wireless Network

After initially loading unit configuration using keys, the EquipCommand software allows you to update unit configuration information over the wireless network.

To load unit configurations over the wireless network:

1. In the Unit Setup menu, click Send Configuration via Radio.

   The Send Configuration via Radio window displays.



2. Select the appropriate entries in the four list boxes.

   Refer to the table below for a description of the list boxes.

Send Configuration via Radio List Boxes	Description
Units	Units to which a configuration can be sent. You can use Ctrl+click and Shift+click to select multiple units.
List Type Settings	Select the type of settings or information to send to the selected units: • Events Requiring Location. Settings that provide location information for events. For information about creating custom events, refer to "Creating Custom Events" on page 54. • Firmware Upgrade. The ImpactManager RF operating code. • Input Configuration. A list of configuration settings that define how the ImpactManager RF inputs function. • Operator List. A list of operators who have been given authorization to operate a particular unit. • Safety Checklist. The list of questions that are presented to an operator during a safety check. • Operator Pre-Defined Messages. The list of pre-defined messages. • Operator Daily Checklist. The daily safety checklist for the operator. **NOTE:** Any untrained person who uses this feature to upgrade the firmware over the air could erase all settings of a unit.
Single Setting Item	Select from the list of single items of information or settings to send to the selected units.
Command/Request	Select a command or request to send to the selected units.

3. When finished selecting items in the List Type Settings, Single Setting Item, or Command/Request list, click the Send button below the list to send the selected information.

   -OR-

   If you have selected information in more than one list, click the Send All Settings button to send all the selected configurations.

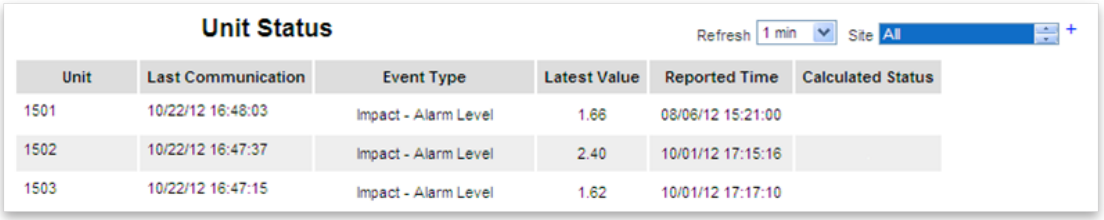
Section 7. System Monitoring

7.1 Unit Status

The current status for any unit that has been identified to the EquipCommand software can be found on the Unit Status window.

To access the Unit Status window, in the System Status menu, click Status Monitoring.

The Unit Status window displays.



Unit	Last Communication	Event Type	Latest Value	Reported Time	Calculated Status
1501	10/22/12 16:48:03	Impact - Alarm Level	1.66	08/06/12 15:21:00	
1502	10/22/12 16:47:37	Impact - Alarm Level	2.40	10/01/12 17:15:16	
1503	10/22/12 16:47:15	Impact - Alarm Level	1.62	10/01/12 17:17:10	

Each unit that has been identified to the software is listed on this window. The Last Communication column shows the time and date that a particular unit communicated with the software as of the last upload of information from the Yellow Manager's Key. If the word NEVER is displayed, communications between the unit and the software have not occurred.

If a unit had previously communicated with the software, the color of the text in the Last Communication column will be meaningful.

- If the color is Yellow, communications have not occurred within two days.
- If the color is Red, communications have not occurred in four days.

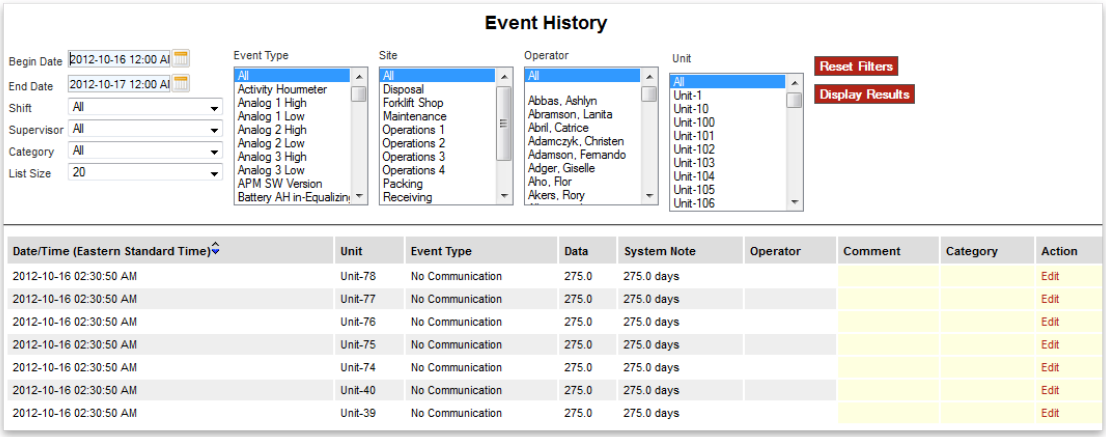
If specific events regarding timers and counters have been set up as described in "Event Alerts Setup Wizard" on page 49, these events are listed per unit, along with the current status of each event.

7.2 Event History

You can view a list of all events generated by ImpactManager RF.

To view the event history, in the System Status menu, click Event History.

The Event History window displays.



Filtering the Event History List

By default, only events generated on the current day are listed.

However, you can display other sets of events using the following filter parameters:

- Date Range
- Shift
- Supervisor
- Category
- Event Type
- Unit Name
- Site
- Operator
- Unit

To filter the event list:

1. Enter/select one or more of the filter parameters.
2. In the List Size field, enter the number of events to return in the filtered results.
3. Click the Display Results button.

   The Event History window refreshes and displays only events that match the selected filter parameters.

To clear the filters, click the Reset Filters button.

Adding a Comment to an Event Entry

Comments can be added to any event in the database.

To add a comment:

1. Click the event entry's Edit link.

   A Comment field and Category list display.

2. Enter your comment in the Comment field.

   You can enter up to 256 characters.

3. Select the appropriate Category.
4. Click the Save link in the Action column.

7.2.1 Pre-Defined Event Types

The Event History window includes a list of Event Types. The system includes pre-defined event types. Refer to the following table for a description of these pre-defined event types.

NOTE: You can also create your own custom events. For the procedure, refer to "Creating Custom Events" on page 54.

Pre-Defined Event	Description
Blocked Key	Generated when an iButton listed on the Blocked Key list is used
Brownout	Generated when power is disconnected for a period longer than the Brownout timer
Certification Expiring	Generated when an operator's certification will be expiring shortly
Condition Not Met	Generated when data was received that indicates an expected condition was not met
Data Received	Generated to record data received that is not an event; for example, the firmware version of the unit
Firmware Downloaded	Generated when new firmware has been downloaded to the unit

Pre-Defined Event	Description
Fuse Failure	Generated when the external connection fuse has failed
Fuse Normal	Generated when the external connection fuse is normal
Impact – Alarm Level	Generated when an impact exceeds Alarm threshold
Impact – Vertical	Generated when an impact in the vertical plane occurs
Impact – Warning Level	Generated when an impact exceeds Warning threshold
Impact Sensor Disconnected	Generated when the external impact sensor is disconnected from the 24-Pin Terminal Strip
Impact Sensor Normal	Generated when the external impact sensor is reconnected to the 24-Pin Terminal Strip
Inspection	Generated when Blue Maintenance key is applied to the unit
Lockout/Tagout	Generated when Blue Maintenance key is held in place for three seconds
Maintenance Due	Generated when Maintenance Due timer expires
Maintenance Log OFF	Generated when a maintainer has logged off
Maintenance Log ON	Generated when a maintainer has logged on
Maintenance Timer Reset	Generated when Blue Maintenance key is applied while the Maintenance Timer has expired
Managers Key	Generated when Yellow Manager's Key is applied to collect data
Maximum Exceeded	Generated when a value is above an expected maximum
Microsoft Error Code	Generated for debugging purposes
Midnight Break	Generated when an operator is logged on to a unit and operation passes into a new day
Minimum Not Met	Generated when a value is below an expected minimum
Module Reset	Generated when ImpactManager RF hardware has restarted
Operator List Received	Generated when a unit successfully receives an new Operators list
Operator Log Off	Generated when an operator logs off the unit
Operator Log On	Generated when an operator logs on to the unit
Reset Shutdown Mode	Generated when a Yellow Manager's key or a Black Reset key is used to reset a unit out of shutdown mode
Reset Wakeup	To be defined for future use
Settings	Generated when a Red Settings key is used

Pre-Defined Event	Description
System Error	Generated when there is a system error and status condition occurs (not always an error)
System Log Off	Generated when the unit has logged off the operator (normally due to inactivity)
Test Event	Generated to convey hardware debugging information
UnLock	Generated when a Blue Maintenance key unlocks a unit from lockout/tag out mode
Voltage Low	Generated when the monitor voltage level goes under the preset threshold for longer than the preset time
Voltage OK	Generated when voltage monitoring is used and the voltage level has returned to normal

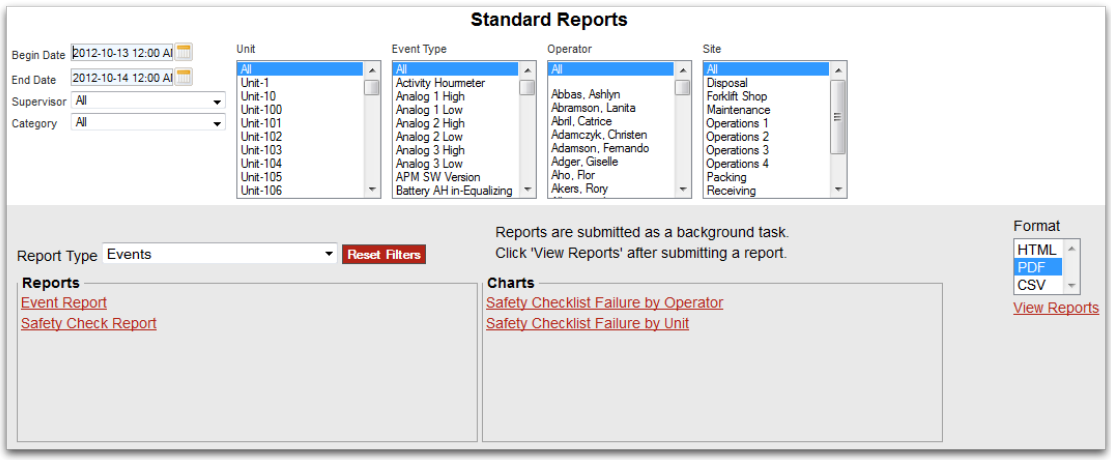
Section 8. Reports

The EquipCommand software includes standardized reports.

To access EquipCommand reports:

1. In the System Status menu, click Standard Reports.

   The Standard Reports window displays.



   Reports are categorized by three primary parameters: Utilization, Events, and Impacts.

2. Use the Date fields and lists at the top of the window to enter filter criteria for the report.

   The date defaults to the current date and time. To reset the filters, click the Reset Filters button.

3. Select the file format for the report in the Format list.

   Reports can be produced in HTML, PDF, or CSV. HTML reports are rendered by a web browser. PDF files are rendered by Adobe Acrobat. CSV files are rendered by your web browser but are compatible with other applications such as Excel, Access, etc.

4. Choose a report type in the Report Type list.

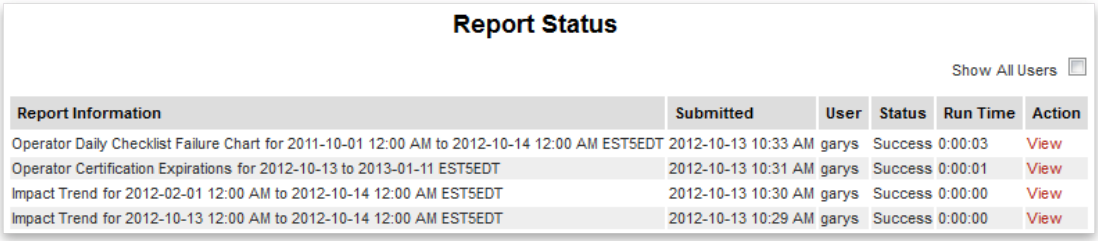
The available reports and charts change depending on the report type selected.

5. To generate a report or chart, click its link.

   A message displays indicating that the report has been submitted.

6. Click the OK button to dismiss the message.
7. To view the reports that have been generated, click the View Reports link.

   The Report Status window displays.



Report Status

Show All Users ☐

Report Information	Submitted	User	Status	Run Time	Action
Operator Daily Checklist Failure Chart for 2011-10-01 12:00 AM to 2012-10-14 12:00 AM EST5EDT	2012-10-13 10:33 AM	garys	Success	0:00:03	View
Operator Certification Expirations for 2012-10-13 to 2013-01-11 EST5EDT	2012-10-13 10:31 AM	garys	Success	0:00:01	View
Impact Trend for 2012-02-01 12:00 AM to 2012-10-14 12:00 AM EST5EDT	2012-10-13 10:30 AM	garys	Success	0:00:00	View
Impact Trend for 2012-10-13 12:00 AM to 2012-10-14 12:00 AM EST5EDT	2012-10-13 10:29 AM	garys	Success	0:00:00	View

8. By default, only the operators and sites to which you have access are included in reports. To include the information that is available to all EquipCommand report users, select the All Users option.
9. To view one of the completed reports, click its View link.

   You are prompted to open the report or save it in the file format that you chose.

8.1 Available Reports and Charts

8.1.1 Events Reports

Event Report

A general, user-customizable report that can present a single event, a selection of events, or all events over a selected span of time, units, operators, models, and sites.

Safety Check Report

Provides only safety checklist-related event data. Successful safety checklist completions, critical safety checklist failures, non-critical safety checklist failures, and safety checklist reset/bypass events are presented. Standard filtering options (date, operator, site) apply.

NOTE: This report is not supported for ImpactManager RF.

Safety Checklist Failure By Operator (Chart)

Presents a bar chart reflecting the total number of safety checklist failures (both critical and non-critical) for each operator over the filtered selection (date, operator, site).

NOTE: This report is not supported for ImpactManager RF.

Safety Checklist Failure by Unit (Chart)

Presents a bar chart reflecting the total number of safety checklist failures (both critical and non-critical) for each unit over the filtered selection (date, operator, site).

NOTE: This report is not supported for ImpactManager RF.

8.1.2 Utilization Reports

All Utilization reports are based on the comparison of total "log-on" time to total "active" time. Log-on time is calculated by measuring the time between operator login and operator logout. Active time is reported as the amount of time within each operator's login time that the equipment was actually moving, as measured by the unit mounted motion sensor.

Utilization by Operator

Provides overall utilization data, per operator, over the filtered selection. Overall time logged in, overall time Active (based upon motion sensor, or activity line for EquipManager/FleetControl Manager), and the percentage of time Active.

Utilization by Unit

Provides overall utilization data, per unit, over the filtered selection. Overall time logged in, overall time Active (based upon motion sensor, or activity line for EquipManager/FleetControl Manager), and the percentage of time Active.

Unit Time Analysis

Provides detailed information on the usage of the unit. Time logged on, logged off, active, idle, as well as percentages of each are included.

Operator Utilization Summary

Provides detailed data regarding selected operators' usage of the equipment. The report reflects each operator's log in/log out duration and the overall utilization of that span.

Unit Utilization Summary

Provides detailed data regarding selected unit usage. The report reflects each units log in/log out duration and the overall utilization of that span.

Utilization Chart by Operator (Chart)

Presents a bar chart displaying operator active/inactive time.

Utilization Chart by Unit (Chart)

Presents a bar chart displaying unit active/inactive time.

Operator Usage Scale (Chart)

Presents a chart listing hours of utilization within a selected time period, per operator, from least utilized to most.

Unit Usage Scale (Chart)

Presents a chart listing hours of utilization within a selected time period, per unit, from least utilized to most.

8.1.3 Impact Reports

NOTE: All Impact reports involve the impact or events.

Impact Frequency by Operator

Provides operator impact information over a selected period of time (in hours). Shows how many impacts each operator had within that window of time, and breaks it down to "hours per hit", allowing management to see who generates impacts more frequently across the operator group.

Impact Frequency by Unit

Provides unit impact information over a selected period of time (in hours). Shows how many impacts each unit had within that window of time, and breaks it down to "hours per hit", allowing management to see who generates impacts more frequently across the equipment group.

Operator Impact Summary

Provides a summary of impact events (both warning and alarm level) for each operator, listing both the number of impacts and the severity.

Unit Impact Summary

Provides a summary of impact events (both warning and alarm level) for each unit, listing both the number of impacts and the severity.

Impact by Operator (Chart)

Presents the total number of impacts, per operator, over a selected span of time in bar chart format.

Impact by Unit (Chart)

Presents the total number of impacts, per unit, over a selected span of time in bar chart format.

Impact by Supervisor (Chart)

Presents the total number of impacts, per supervisor (via their direct operators), over a selected span of time in bar chart format.

Impact by Site (Chart)

Presents the total number of impacts, per site, over a selected span of time in bar chart format.

Impact by Model (Chart)

Presents the total number of impacts, per equipment model, over a selected span of time in bar chart format.

Impact Trend (Chart)

Presents a line chart reflecting the total number of impacts over a span of time (i.e., week to week, month to month), providing impact trend data.

8.1.4 Operator Certification Expiration Report

Provides a list of operators whose certification is set to expire.

8.1.5 Simultaneous Utilization Report

Presents a multi-line chart that reflects the total number of trucks in the fleet, and how well utilized the entire fleet is over a span of time. Helpful for right-sizing fleets.

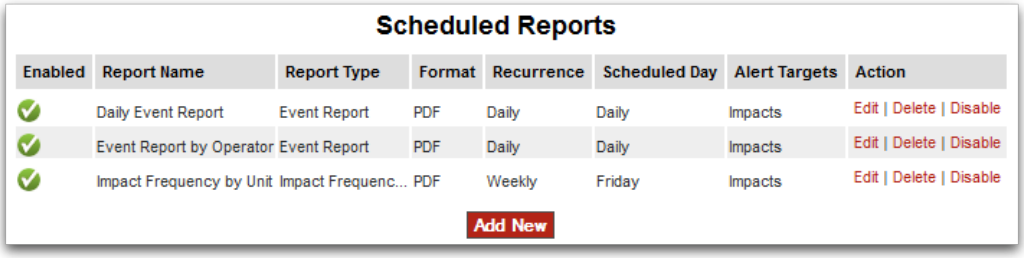
8.2 Scheduled Reporting

EquipCommand provides the ability to schedule reports for automated delivery via e-mail. Any report currently available in the EquipCommand software suite is available for automated delivery.

Viewing the List of Scheduled Reports

To view the list of scheduled reports, in the Software Setup menu, click Scheduled Reports.

The Scheduled Reports window displays.



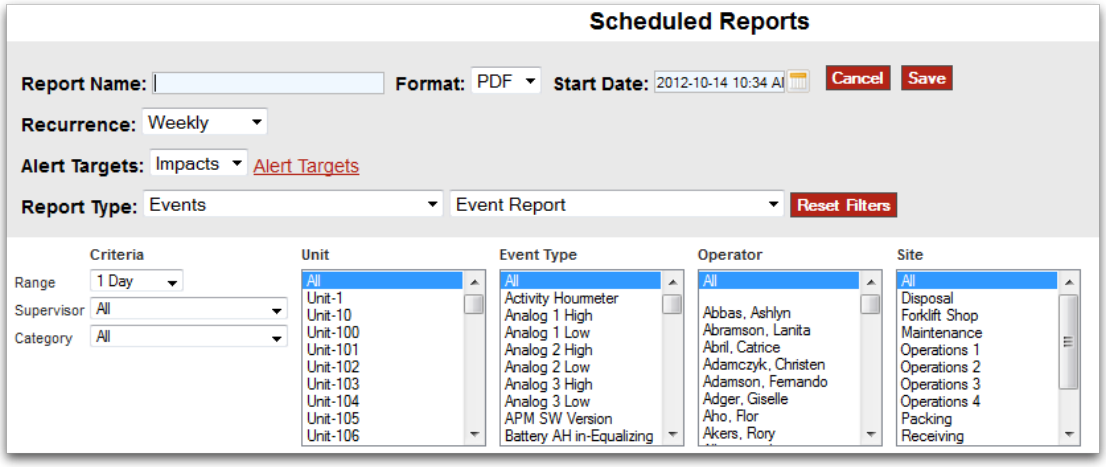
Any report in the list can be edited, deleted, or disabled/enabled by clicking the appropriate link in the Action column.

Adding a Scheduled Report

To add a schedule report:

1. Click the Add New button.

   The Scheduled Reports - Add New window displays.



2. Complete the report parameters and filters for the report data.

   The report parameters and filters are different for each report type. The following table describes the parameters and filters for an Events report.

Scheduled Report Parameters and Filters	Description
Report Name	The name of the report. This will appear on the Scheduled Reports window.
Format	The file format—either PDF or CSV—for the report.

Scheduled Report Parameters and Filters	Description
Start Date	The date and time at which the report data collection will begin. The report will then be generated according to the frequency specified in the Recurrence list and delivered on the next closest hour to the time specified. Data is collected from midnight to midnight. For example, if the start date and time is November 5, 2012 at 8:12 am and the Recurrence is set to Weekly, then the first report data collection will start just after midnight on November 5 and will end at November 11, 2012 at midnight. The report will be delivered on November 12 at 9:00 am.
Recurrence	The frequency at which the report will be generated.
Alert Targets	**NOTE:** Alert Targets do not apply to ImpactManager RF.
Report Type	The genre of report to run, as well as the specific report type.
Range	The period of time the report will capture.
Supervisor	The supervisor whose operators will be included in the report (provided that operators are assigned to the supervisor).
Category	Filters events by a specific category (if events are assigned to that category).
Unit	Select the units to be included in the report.
Operator	Select the operators to be included in the report.
Site	Select the sites to be included in the report.

3. When finished, click the Save button to save the schedule report.

   The Scheduled Reports window displays and the new scheduled report is added to the list.

NOTE: Reports are not generated automatically, but according to the settings selected.

Section 9. System Utilities

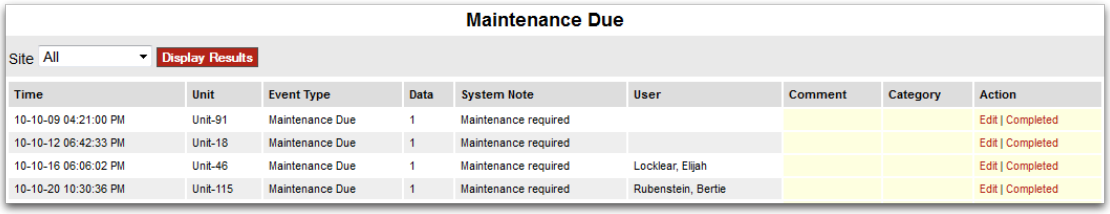
9.1 Maintenance Due Report

The EquipCommand software provides an online Maintenance Due report that allows you to track when units requires maintenance, as configured with the Maintenance Timer settings. For information about this setting, refer to "Maintenance and Voltage Monitoring" on page 32.

When a unit's Maintenance Timer expires, a Maintenance Due event is generated. The name of this unit is then be listed in the Maintenance Due report. Once a unit is listed, it can be removed by generating a Maintenance Timer Reset event at the unit or by clicking the Maintenance Due entry's Completed link in the Maintenance Due window. The receipt of this event cancels the Maintenance Due event, and the unit listing is removed from the Maintenance Due report.

Viewing the Maintenance Due Report

To view the Maintenance Due report, in the System Status menu, click Maintenance Due Check. The Maintenance Due window displays.



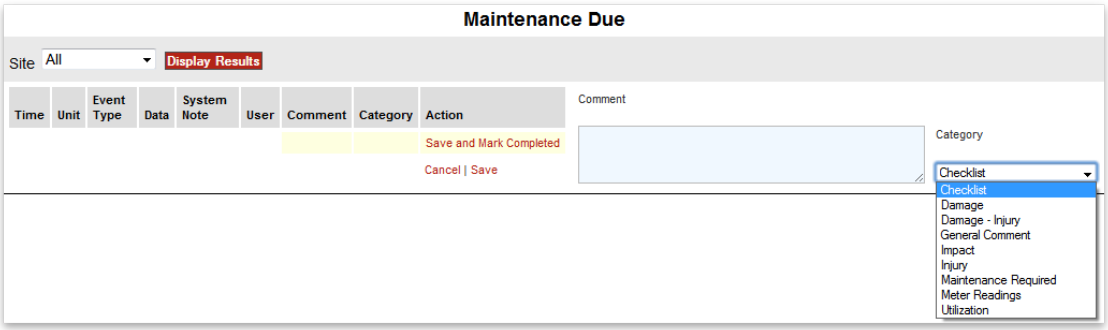
To edit or mark a maintenance entry as Completed, click the appropriate link in the Action column for that entry.

Adding a Comment and Selecting a Category for a Maintenance Due Entry

To add a comment to and select a category for an entry in the Maintenance Due Report:

1. Click the entry's Edit link.

   The Maintenance Due - Edit window displays.



2. Enter a comment about the entry.
3. Select a category for the entry.
4. When finished, click the Save link in the Action column to save the comment and category selection.

   - OR -

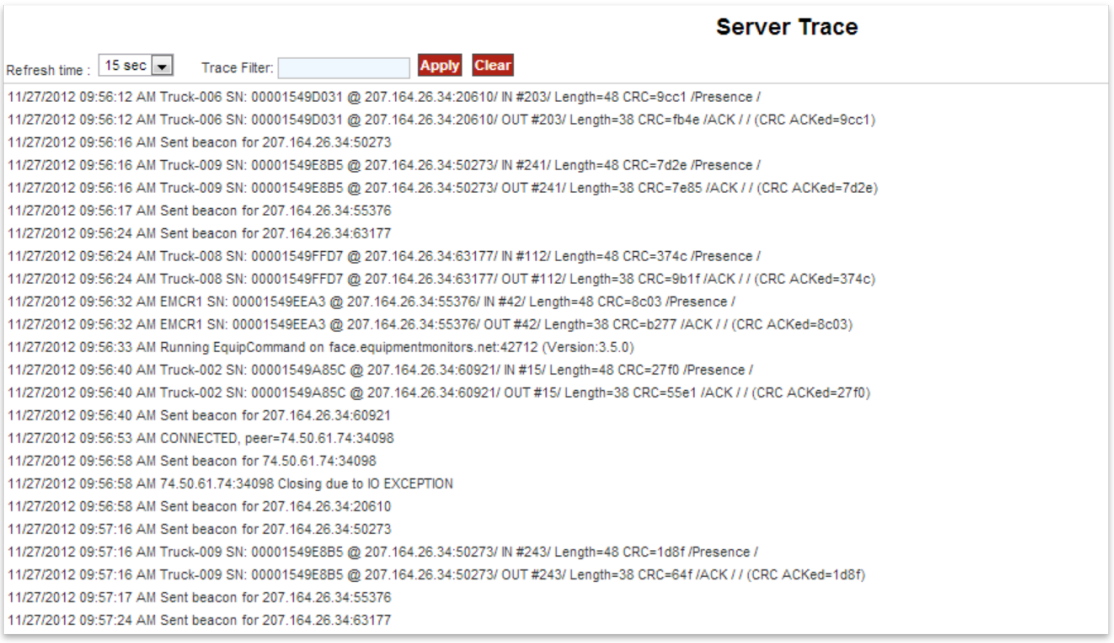
   To save the comment and category, and mark the maintenance as Completed, click the Save and Mark Completed link in the Action column.

9.2 Server Trace

To view a list of all radio transactions sent between the EquipCommand server and the units, in the System Status menu, click Server Trace.

The Server Trace window displays.

The radio transactions that have been sent are listed in the window. By default, the listing is unfiltered and all transactions are included.



To search for an entry in the transaction list, such as a particular unit:

1. Enter search criteria in the Trace Filter field.
2. Click the Apply button.

   The list refreshes and displays only the transactions that include text that matches your search criteria.

To delete your search criteria and refresh the list, click the Clear button.

To specify how often the Server Trace window refreshes, select the time interval from the Refresh Time list.

To temporarily stop the window from refreshing, click the Pause button.

To resume refreshing, click the Resume button.

9.3 E-mailing Log Files to TotalTrax

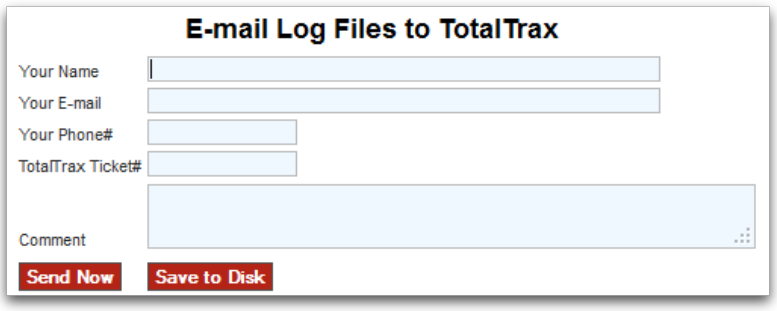
The E-mail Log Files to TotalTrax utility allows you to easily e-mail TotalTrax software log files to TotalTrax technical support if you encounter problems.

NOTE: To use this feature, the PC running the TotalTrax software must be connected to the Internet and have the capability to send e-mails.

To e-mail log files to TotalTrax:

1. In the System Status menu, click E-mail Log Files to TotalTrax.

   The E-mail Log Files to TotalTrax window displays.



2. Complete the e-mail fields.

NOTE: TotalTrax technical support will provide you with a Ticket number.

3. To send the e-mail with log files to TotalTrax, click the Send Now button.

   - OR -

   To save the log files in a Zip file to your local disk so that you can send them to TotalTrax using another method, click the Save to Disk button.

9.4 Displaying System Information

To display information about the system, double-click the version number on the left side of the red menu bar. The System Information page displays. It includes configuration information about your EquipCommand system.

9.5 Tool Tips

Tool tips can be displayed throughout the EquipCommand software. The tips identify a function or process or provide additional description.

The tips are displayed when the mouse cursor is positioned on a particular word, or group of words, for a period of one second. The tip displays as a message box and remains open for 5 seconds.

Section 10. Dashboard Configuration

The TotalTrax EquipCommand Dashboard is a live, user-configurable, snapshot of your fleet. Anything from Utilization to Impacts, Safety Check Failures to Best Drivers, can be tracked and viewed effortlessly.

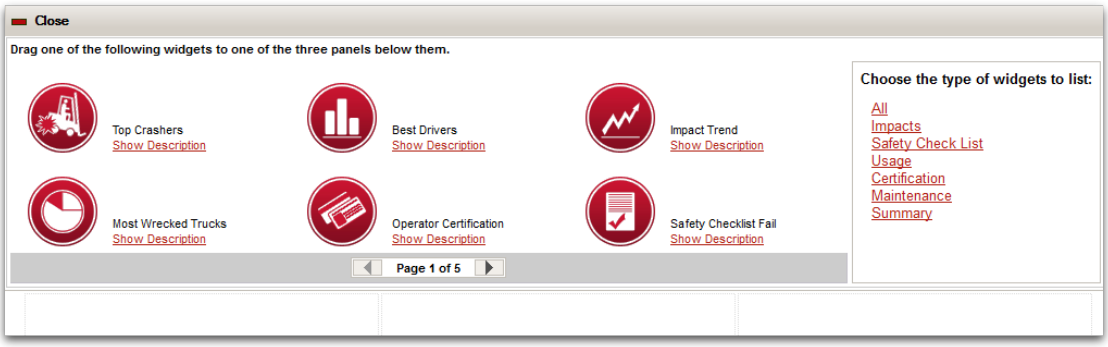
This is accomplished via the Dashboard Widgets. Each widget has a specific purpose and can be configured in a number of ways. Each user with a login to the EquipCommand software has their own Dashboard with their own Widgets, allowing anyone to track the data that means the most to them.

To configure the Dashboard:

1. Click the Dashboard button at the upper left corner of the EquipCommand window.
2. Click the Add Content button at the upper left corner.

   The following window displays the various Widgets from which you can choose.

NOTE: To display a detailed description of a Widget, click its Show Description link.

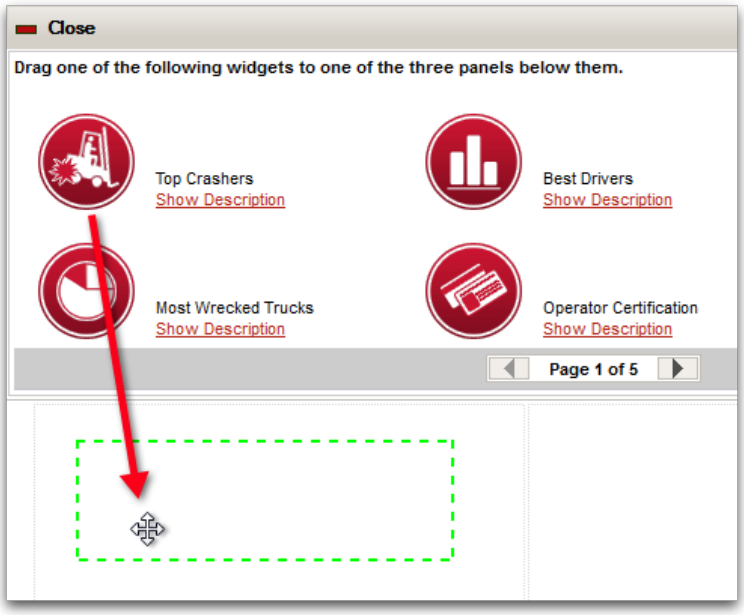


3. To select a Widget, click and drag its icon into the lower (blank) portion of the window, as shown below.

   - OR -

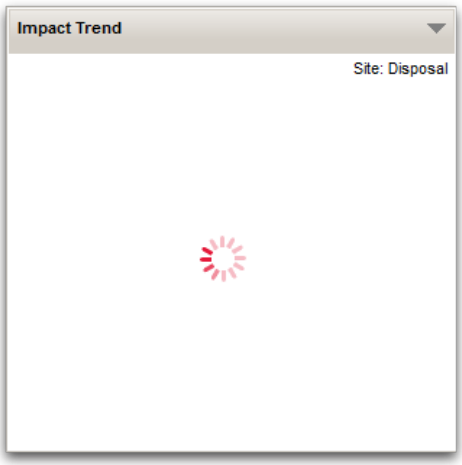
   Double-click the widget.

When dragging a widget, a green outline is shown if the widget is allowed in that space (a black outline indicates that the widget cannot be placed there).



When double-clicking a widget, it is automatically added to the next open space.

Once placed, the widget appears in full, and begins loading its data according to the default settings.



You might want to see different data than that shown using the default settings.

To personalize the data for your widget:

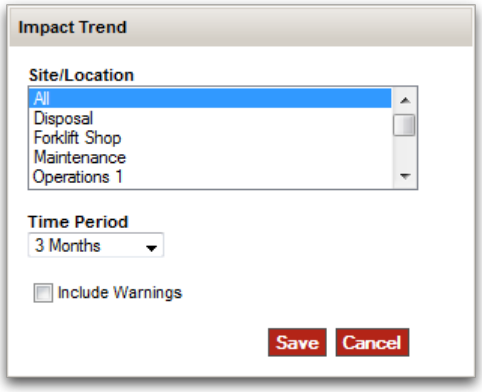
1. Click the down arrow in the top right corner of the widget.

   A menu displays.

2. To change the options, click Settings.

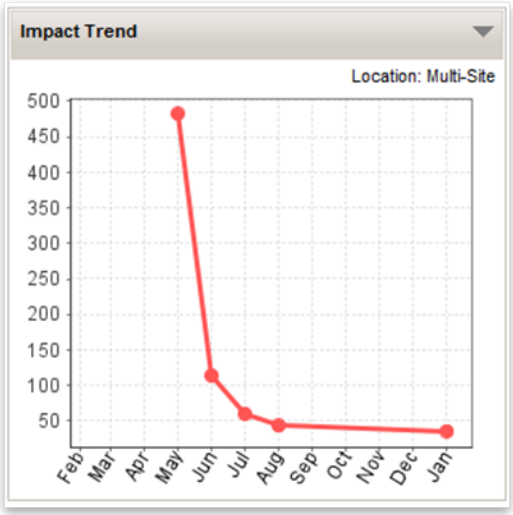
   The available options for the selected Widget display. Widgets have different options depending on the type. For example, an Impact widget has impact-related options and a Utilization widget has options to sort by operator, unit, or other criteria).

   The options for the Impact Trend Widgets are shown below.



3. Select the options you want to use, then click the Save button.

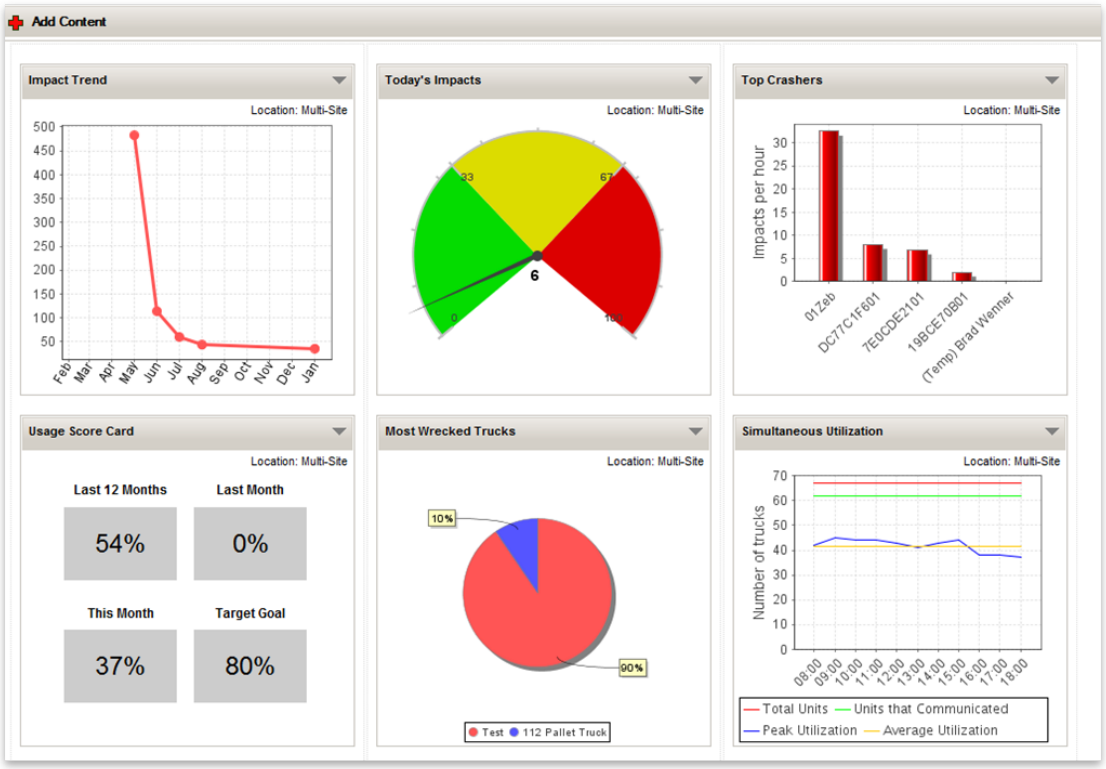
   The Widget automatically repopulates according to the new settings.



   Hovering over the Widget displays a pop-up description of its current settings.

To move your new configured Widget, simply click and drag it to a different location on the lower portion of the window, depending on your preferences.

Feel free to add additional Widgets to customize the Dashboard to fit your needs.


Add Content
Impact Trend
Location: Multi-Site
500
450
400
350
300
250
200
150
100
50
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Today's Impacts
Location: Multi-Site
33
67
6
0
Top Crashers
Location: Multi-Site
Impacts per hour
30
25
20
15
10
5
0
01Zeb
DC77C1F601
7E0CDE2101
19BCE70B01
(Temp) Brad Wenner
Usage Score Card
Location: Multi-Site
Last 12 Months
54%
Last Month
0%
This Month
37%
Target Goal
80%
Most Wrecked Trucks
Location: Multi-Site
10%
90%
Test
112 Pallet Truck
Simultaneous Utilization
Location: Multi-Site
Number of trucks
70
60
50
40
30
20
10
0
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
Total Units
Units that Communicated
Peak Utilization
Average Utilization

Section 11. Database Backup Configuration

EquipCommand allows you to automatically back up its default MySQL database at selected intervals. It is strongly advised that you back up the EquipCommand database regularly to prevent data loss in the event of a catastrophic server failure. Refer to the following procedure to configure the automated backup utility.

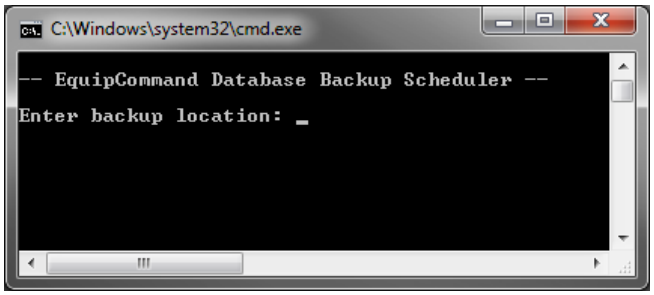
11.1 Configuring an Automated Backup of the EquipCommand Database

1. To configure automated backup of the EquipCommand Database:
2. On the EquipCommand server computer, browse to the EquipCommand scripts folder. It is typically C:\EquipCommand3xx\swserver\scripts.
3. Edit the backupEnv.cmd file to enter the backup schedule information. For example, the following entry would cause the backup to be performed every day at 2:00 am.

   ```
   set BACKUP_TIME=02:00:00
   ```

4. Make sure that the backup device is mounted and that the destination backup folder exists.
5. In the EquipCommand folder, go to the folder \swserver\scripts.
6. Double-click the file ScheduleBackups.cmd.

   A command window opens, prompting for the backup location.



7. Enter the full file path of the backup folder (e.g., D:\Documents\BackedupData, then press the Enter key.

   You are prompted for the password of the logged in Windows user.

8. Enter your Windows password and press the Enter key.
9. In the command window, press any key.

   The command window closes and the backup has been scheduled.

Appendix A. iButton Keys and LED Status Indications

This appendix includes reference information about:

- iButton key definitions and verification sounds
- The iButton reader LED and what the status that it indicates

A.1 iButton Key Definitions and Verification Sounds

Key		Event	Verification Sounds
Green Key (Operator Key)		Operator Log In	1 chirp
		Operator Log Out	2 chirps
		Safety Check in Progress	Warble
Yellow Key (Manager Key)	Data Retrieval	Retrieval Begins	1 chirp
		Retrieval Ends	2 chirps
	Operator List	Transfer Begins	1 chirps
		Transfer Ends	2 sets of 2 chirps
Black Key (Resetter Key)		Reset alarm/ shutdown	1 chip, 1 second, 2 chirps
Red Key (Settings Key)		Programming Complete	3 chirps
Blue Key (Maintainer Key)		Inspection Event	1 chirp
		Lockout	1 chirp, 3 seconds, 1 chirp
		Release/Unlock	1 chirp
		Communication Error	Warble

A.2 iButton Reader LED Status Indications

The ImpactManager RF unit includes an LED on the iButton reader that indicates the status of the unit, as described in the following table.

LED Indications	Status
1 flash every three seconds	No impact data recorded
2 flashes every three seconds	Impact data recorded
3 flashes every three seconds	Memory full
4 flashes every three seconds	Error
5 flashes every three seconds	Radio not detected
LED on with flashes off	Operator logged on
LED off with flashes on	Operator logged off
LED one second on, one second off intervals	Unit locked out

TotalTrax, Inc. Warranty Policy

A limited one-year warranty ("Warranty Period") is standard with all TotalTrax, Inc. units and software. The Warranty Period begins on the date of product shipment. Repair for functional failures and/or cosmetic touch up for units out of warranty is available on a time and materials basis. Software patches and upgrades are available via our web site at www.totaltraxinc.com.

Terms of One-Year Limited Warranty

TotalTrax, Inc. warrants that during the Warranty Period each unit will be:

1. Free from defects in materials and workmanship
2. In compliance with its specifications

If a unit does not function as warranted during the prescribed Warranty Period, return the unit to TotalTrax, Inc. and we will repair or replace it free of charge (see return policy below). THIS IS YOUR SOLE AND EXCLUSIVE REMEDY AND TOTALTRAX, INC. SOLE AND EXCLUSIVE OBLIGATIONS HEREUNDER.

Misuse, accident, modification, cosmetic disfigurement, unsuitable physical operating environment, failure caused by third party products not provided by TotalTrax, Inc. or mishandling may void the warranty.

EXCEPT AS OTHERWISE PROVIDED HEREIN AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, TOTALTRAX, INC. EXPRESSLY DESCLAIMS ALL IMPLIED WARRANTIES, TERMS OR CONDITIONS OF SATISFACTORY QUALITY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NONINFRINGEMENT.

Return Policy

PRIOR TO UNINSTALLING THE UNIT,
PLEASE CALL OUR TECH SUPPORT OFFICE FOR DIAGNOSIS

Prior to shipping a damaged unit or corrupt software to TotalTrax, Inc. for repair or service, contact our Technical Support (855)-895-7720 between 7:00 a.m. to 5:00 p.m. CST, Monday - Friday. to provide a detailed explanation of the problem and receive a Return to Manufacturer Authorization (RMA) number and form. The RMA must be noted in the left-hand corner of the address side of the package. Please repackage the units carefully and include a proper return address and contact name especially if the unit is to be shipped to a field office. Send all materials freight prepaid to the following address:

TotalTrax, Inc.
Technical Services Center
Attn: Repairs
500 Water Street
Newport, DE 19804

All non-warranty maintenance and repair charges will be based upon time and materials, with a minimum charge of $45.00 per unit. If a unit under warranty cannot be repaired, TotalTrax, Inc. reserves the right to replace the unit. The replaced unit may not be new but will be in good working order. Prior to service or repair, TotalTrax, Inc. will notify you of any non-

warranty costs involved and will not begin such repairs until a purchase order is received from you. All warranted repairs will be returned at TotalTrax, Inc. expense.

Technical Support

TotalTrax, Inc. Technical Support is provided free of charge at the following telephone numbers.

T: (855)-895-7721
F: (940)-549-0674

Technical support business hours are 7:00 a.m. to 5:00 p.m. CST, Monday - Friday.

End User License Agreement

FOR TOTALTRAX EQUIPMENT MONITOR SOFTWARE

IMPORTANT-READ CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between the person, company, organization or other entity that has licensed this software (“You” or “Customer”) and TotalTrax, Inc. (“TotalTrax”) for the TotalTrax Software that accompanies this EULA (referred to herein as "Software"). An amendment or addendum to this EULA may accompany the Software. YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA BY INSTALLING, COPYING, OR USING THE SOFTWARE. IF YOU DO NOT AGREE, DO NOT INSTALL, COPY, OR USE THE SOFTWARE. YOU MAY RETURN IT TO YOUR PLACE OF PURCHASE FOR A FULL REFUND, IF APPLICABLE.

THIS EULA SHALL APPLY ONLY TO THE SOFTWARE SUPPLIED BY TotalTrax HEREWITH REGARDLESS OF WHETHER OTHER SOFTWARE IS REFERRED TO OR DESCRIBED HEREIN. 1. GRANT OF LICENSE. TotalTrax grants You the following rights provided that You comply with all terms and conditions of this EULA:

1.1 Installation and use. You may install and use the Software on one or more personal computers or network storage devices, such as server computers. The personal computers or network storage devices need not be at a single location. The Software is designed to interact with equipment monitors located on equipment such as material handling equipment. The Software is only licensed for use only by the legal entity that operates the equipment monitors and operates the equipment that is monitored by the equipment monitors. The Software is not licensed for use with equipment monitors owned or operated by, or for equipment operated by, an entity other than You; a separate license is required from TotalTrax.

1.2 License Grant for Documentation. The documentation that accompanies the Software is licensed for internal reference purposes only.

1.3 Permission to Conduct Audit. You agree that TotalTrax may audit Your use of the Software for compliance with these terms at any time, upon reasonable notice. In the event that such audit reveals any use of the Software by You other than in full compliance with the terms of this Agreement, You shall reimburse TotalTrax for all reasonable expenses related to such audit in addition to any other liabilities You may incur as a result of such non-compliance.

1.4 License Rights are Non-Exclusive. Your license rights under this EULA are non-exclusive.

2. NO RENTAL/COMMERCIAL HOSTING. You may not rent, lease, lend or provide commercial hosting services with the Software.

3. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

3.1 Mandatory Activation. THERE MAY BE TECHNOLOGICAL MEASURES IN THIS SOFTWARE THAT ARE DESIGNED TO PREVENT UNLICENSED USE OF THE SOFTWARE. You may not be able to exercise your rights to the Software under this EULA after a finite number of product launches unless You activate your copy of the Software in the manner described during the launch sequence of the Software. You may also need to reactivate the Software if You modify your computer hardware or alter the Software. TotalTrax will use those measures to confirm You have a legally licensed copy of the Software. If You are not using a licensed copy of the Software, You are not allowed to install the Software or future Software updates. TotalTrax will not collect any personally identifiable information from your device during this process.

3.2 Internet-Based Services. The Software may contain components that enable and facilitate the use of certain Internet-based services. You may not use any TotalTrax Internet-based services associated with the Software in any manner that could damage, disable, overburden, or impair such services or interfere with any other party's use and enjoyment of them. You may not attempt to gain unauthorized access to any service, account, computer systems or networks associated with the Internet-based services.

3.3 Report-Writing Runtime Software Limitations. The Software may contain report writing runtime software ("Runtime Software"). Other than use with the Software, You may not use the Runtime Software with any other software application nor use the Runtime Software as part of any process or system that is used to automatically deliver, share or distribute documents or other work created using the Runtime Software.

4. RESERVATION OF RIGHTS AND OWNERSHIP. TotalTrax reserves all rights not expressly granted to You in this EULA. The Software is protected by copyright and other intellectual property laws and treaties. TotalTrax owns the title, copyright, and other intellectual property rights in the Software. The Software is licensed, not sold. This EULA does not grant You any rights to trademarks or service marks of TotalTrax.

5. LIMITATIONS ON REVERSE ENGINEERING, DECOMPILATION, AND DISASSEMBLY. You may not reverse engineer, decompile, or disassemble the Software, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.

6. CONSENT TO USE OF DATA. You agree that TotalTrax and its affiliates may collect and use technical information gathered as part of the product support services provided to you, if any, related to the Software. TotalTrax may use this information solely to improve our products or to provide customized services or technologies to You and will not disclose this information in a form that personally identifies you.

7. LINKS TO THIRD PARTY SITES. The Software may contain links and access to third party sites. TotalTrax is not responsible for the contents of any third-party sites or services, any links contained in third-party sites or services, or any changes or updates to third-party sites or services. TotalTrax is providing these links and access to third-party sites and services to You only as a convenience, and the inclusion of any link or access does not imply an endorsement by TotalTrax of the third-party site or service.

8. ADDITIONAL SOFTWARE/SERVICES. This EULA applies to updates, supplements, add-on components, or Internet-based services components, of the Software that TotalTrax may provide to You or make available to You after the date You obtain your initial copy of the Software, unless they are accompanied by separate terms. TotalTrax reserves the right to discontinue any Internet-based services provided to You or made available to You through the use of the Software.

9. UPGRADES. To use Software identified as an upgrade, You must first be licensed for the software identified by TotalTrax as eligible for the upgrade. After installing the upgrade, You may no longer use the original software that formed the basis for your upgrade eligibility, except as part of the upgraded software.

10. NOT FOR RESALE SOFTWARE. Software identified as "Not for Resale" or "NFR," may not be sold or otherwise transferred for value, or used for any purpose other than demonstration, test or evaluation.

11. EXPORT RESTRICTIONS. You acknowledge that the Software is subject to U.S. export jurisdiction. You agree to comply with all applicable international and national laws that apply to the Software, including the U.S. Export Administration Regulations, as well as end-user, end-use, and destination restrictions issued by U.S. and other governments.

12. SEPARATION OF COMPONENTS. The Software is licensed as a single product. Its component parts may not be separated for use on more than one device.

13. SOFTWARE TRANSFER TO THIRD PARTY. If You are the person who initially licensed the Software, You may make a one-time permanent transfer of this EULA, Software and Certificate of Authenticity (if applicable) to another end user, provided that You do not retain any copies of the Software. This transfer must include all of the Software (including all copies, component parts, the media and printed materials, any upgrades, this EULA, and, if applicable, the Certificate of Authenticity). The transfer may not be an indirect transfer, such as a consignment. Prior to the transfer, the end user receiving the Software must agree to all the EULA terms.

14. TERMINATION. Without prejudice to any other rights, TotalTrax may terminate this EULA if You fail to comply with the terms and conditions of this EULA. In such event, You must destroy all copies of the Software and all of its component parts.

15. LIMITED WARRANTY FOR SOFTWARE ACQUIRED IN THE US AND CANADA. TotalTrax warrants that the Software will perform substantially in accordance with the accompanying materials for a period of fifteen (15) days from the date of receipt ("Limited Warranty"). If an implied warranty or condition is created by your state/jurisdiction and federal or state/provincial law prohibits disclaimer of it, You also have an implied warranty or condition, BUT ONLY AS TO DEFECTS DISCOVERED DURING THE PERIOD OF THIS LIMITED WARRANTY (FIFTEEN DAYS). AS TO ANY DEFECTS DISCOVERED AFTER THE FIFTEEN DAY PERIOD, THERE IS NO WARRANTY OR CONDITION OF ANY KIND. Some states/jurisdictions do not allow limitations on how long an implied warranty or condition lasts, so the above limitation may not apply to you. Any supplements or updates to the Software, including without limitation, any (if any) service packs or hot fixes provided to You after the expiration of the fifteen day Limited Warranty period are not covered by any warranty or condition, express, implied or statutory.

LIMITATION ON REMEDIES; NO CONSEQUENTIAL OR OTHER DAMAGES. Your exclusive remedy for any breach of this Limited Warranty is as set forth below. Except for any refund elected by TotalTrax, YOU ARE NOT ENTITLED TO ANY DAMAGES, INCLUDING BUT NOT LIMITED TO CONSEQUENTIAL DAMAGES, if the Software does not meet TotalTrax's Limited Warranty, and, to the maximum extent allowed by applicable law, even if any remedy fails of its essential purpose. The terms of Section 17 ("Exclusion of Incidental, Consequential and Certain Other Damages") are also incorporated into this Limited Warranty. Some states/jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you. This Limited Warranty gives you specific legal rights. You may have other rights which vary from state/jurisdiction to state/jurisdiction.

YOUR EXCLUSIVE REMEDY. THIS REMEDY IS THE SOLE AND EXCLUSIVE REMEDY AVAILABLE TO YOU FOR BREACH OF EXPRESS OR IMPLIED WARRANTIES WITH RESPECT TO THE SOFTWARE AND RELATED DOCUMENTATION. TotalTrax's and its suppliers' entire liability and your exclusive remedy for any breach of this Limited Warranty or for any other breach of this EULA or for any other liability relating to the Software shall be, at TotalTrax's option from time to time exercised subject to applicable law, (a) return of the amount paid (if any) for the Software, or (b) repair or replacement of the Software, that does not meet this Limited Warranty and that is returned to TotalTrax with a copy of your receipt. You will receive the remedy elected by TotalTrax without charge, except that You are responsible for any expenses You may incur (e.g. cost of shipping the Software to TotalTrax). This Limited Warranty is void if failure of the Software has resulted from accident, abuse, misapplication, abnormal use or a virus. Any replacement Software will be warranted for the remainder of the original Limited Warranty period or thirty (30) days, whichever is longer, and TotalTrax will use commercially reasonable efforts to provide your remedy within a commercially reasonable time of your compliance with TotalTrax's warranty remedy procedures. Outside the United States or Canada, neither these remedies nor any product support services offered by TotalTrax are available without proof of purchase from an authorized international source. To exercise your remedy, contact: TotalTrax Technical Support, 800-466-0101, U.S. only 940-549-4214; 510 Corporate Drive, Graham, Texas 76450, or the TotalTrax distributor serving your country.

16. DISCLAIMER OF WARRANTIES. The Limited Warranty that appears above is the only express warranty made to You and is provided in lieu of any other express warranties or similar obligations (if any) created by any advertising, documentation, packaging, or other communications. Except for the Limited Warranty and to the maximum extent permitted by applicable law, TotalTrax and its suppliers provide the Software and support services (if any) AS IS AND WITH ALL FAULTS, and hereby disclaim all other warranties and conditions, whether express, implied or statutory, including, but not limited to, any (if any) implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of reliability or availability, of accuracy or completeness of responses, of results, of workmanlike effort, of lack of viruses, and of lack of negligence, all with regard to the Software, and the provision of or failure to provide support or other services, information, software, and related content through the Software or otherwise arising out of the use of the Software. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT WITH REGARD TO THE SOFTWARE.

17. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL TotalTrax OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, FOR NEGLIGENCE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE. THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATON, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS EULA, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), MISREPRESENTATION, STRICT LIABILITY, BREACH OF CONTRACT OR BREACH OF WARRANTY OF TotalTrax OR ANY SUPPLIER, AND EVEN IF TotalTrax OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

18. LIMITATION OF LIABILITY AND REMEDIES. Notwithstanding any damages that You might incur for any reason whatsoever (including, without limitation, all damages referenced herein and all direct or general damages in contract or anything else), the entire liability of TotalTrax and any of its suppliers under any provision of this EULA and your exclusive remedy hereunder (except for any remedy of repair or replacement elected by TotalTrax with respect to any breach of the Limited Warranty) shall be limited to the greater of the actual damages You incur in reasonable reliance on the Software up to the amount actually paid by You for the Software or US$100.00. The foregoing limitations, exclusions and disclaimers (including Sections 15, 16 and 17) shall apply to the maximum extent permitted by applicable law, even if any remedy fails its essential purpose.

19. BASIS OF BARGAIN. The Limited Warranty and Disclaimer, Exclusive Remedies and Limited Liability set forth above are fundamental elements of the basis of the agreement between TotalTrax and You. TotalTrax would not be able to provide the Software on an economic basis without such limitations. Such Limited Warranty and Disclaimer, Exclusive Remedies and Limited Liability inure to the benefit of TotalTrax's licensors.

20. APPLICABLE LAW. If You acquired this Software in the United States, this EULA shall be governed and construed in accordance with the laws of the State of Texas and cannot be amended without the written consent of the parties hereto. Venue for all purposes hereunder shall be in Dallas County, Texas. If You acquired this Software in the European Union, Iceland, Norway, or Switzerland, then local law applies. If You acquired this Software in any other country, then local law may apply.

21. ENTIRE AGREEMENT, SEVERABILITY. This EULA (including any addendum or amendment to this EULA which is included with the Software) is the entire agreement between You and TotalTrax relating to the Software and the support services (if any) and they supersede all prior or contemporaneous oral or written communications, proposals and representations with respect to the Software or any other subject matter covered by this EULA. To the extent the terms of any TotalTrax policies or programs for support services conflict with the terms of this EULA, the terms of this EULA shall control. If any provision of this EULA is held to be void, invalid, unenforceable or illegal, the other provisions shall continue in full force and effect.

22. AMENDMENTS. No TotalTrax's dealer, agent, or employee is authorized to make any amendment to this EULA unless such amendment is in writing and signed by a duly authorized representative of TotalTrax.

23. TRADEMARKS. TotalTrax, IMPACT MANAGER, EQUIP MANAGER, USAGE MANAGER and other trademarks contained in the Software are trademarks or registered trademarks of TotalTrax in the United States and/or other countries. Third party trademarks, trade names, product names and logos may be the trademarks or registered trademarks of their respective owners. You may not remove or alter any trademark, trade names, product names, logo, copyright or other proprietary notices, legends, symbols or labels in the Software. This EULA does not authorize you to use TotalTrax or its licensors' names or any of their respective trademarks.

24. COSTS OF LITIGATION. If any action is brought by either party to this EULA against the other party regarding the subject matter hereof, the prevailing party shall be entitled to recover, in addition to any other relief granted, reasonable attorney fees and expenses of litigation.

25. NO WAIVER. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.