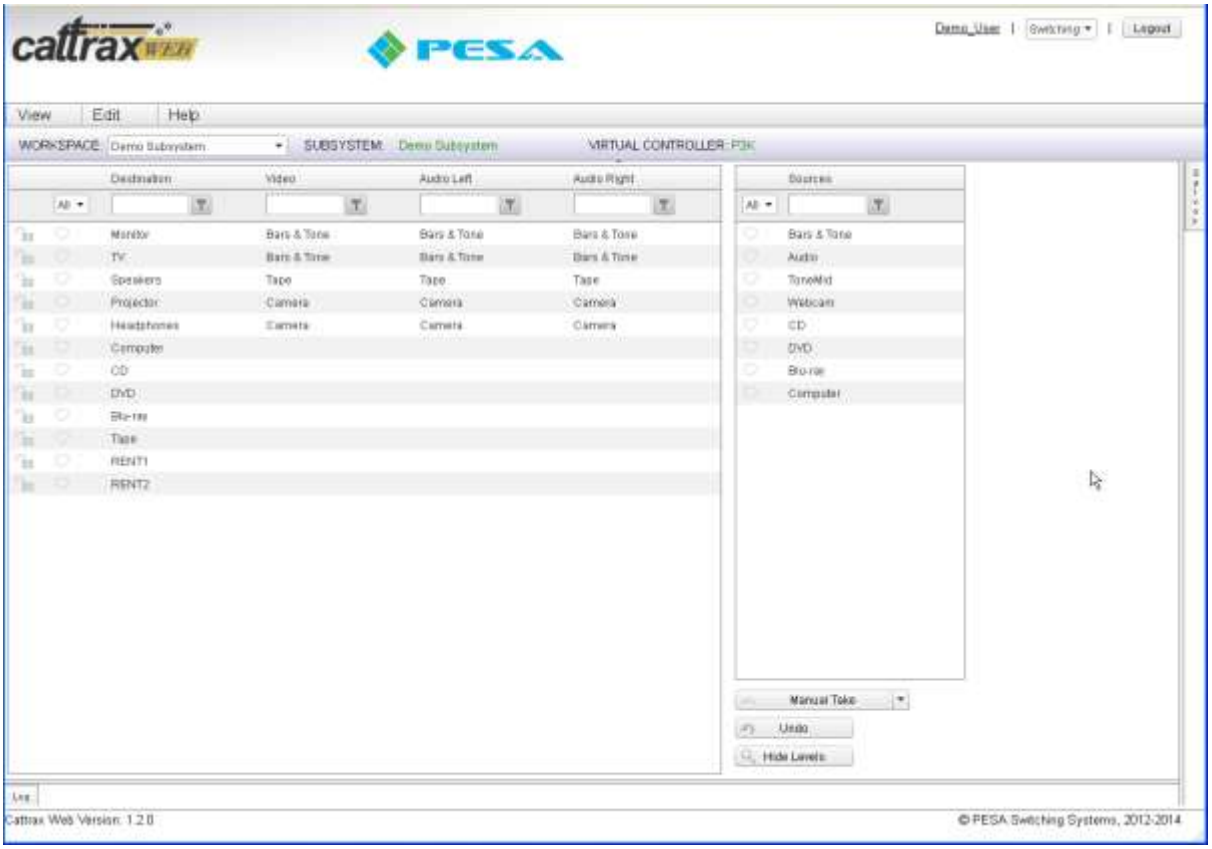
USER GUIDE

WEB-BASED SYSTEM CONTROL APPLICATION



Publication: 81-9059-0703-0, Rev. E
May 2020

www.pesa.com
Phone: 256.726.9200

Thank You for Choosing PESA!!

We appreciate your confidence in our products. PESA produces quality, state-of-the-art A/V processing, routing and distribution equipment designed to deliver our users the highest degree of performance, dependability and versatility available anywhere. If you ever have a question or concern with a PESA product, we have a team of engineers, technicians and customer service professionals available 24/7 every day of the year to help resolve the issue.

Again thank you for choosing PESA, and we look forward to a long-term partnership with you and your facility.

SERVICE AND ORDERING ASSISTANCE
PESA
103 Quality Circle, Suite 210
Huntsville AL 35806 USA
www.PESA.com

MAIN OFFICE
Tel: 256.726.9200
Fax: 256.726.9271

CUSTOMER SERVICE DEPARTMENT
Tel: 256.726.9222 (24/7)
Toll Free: 800.323.7372
Fax: 256.726.9268
Email: service@PESA.com

Printed in the United States of America.

May 2020 – Rev E

March 2018 – Rev D

August 2014 – Rev C

September 2013 – Rev B

October 2012 – Rev A

TABLE OF CONTENTS

CHAPTER 1 ABOUT THIS MANUAL 1-1
1.1 DOCUMENTATION AND SAFETY OVERVIEW 1-1
1.2 CAUTIONS, AND NOTES 1-1
CHAPTER 2 INTRODUCTION 2-1
2.1 DESCRIPTION 2-1
2.2 ALTERNATE LOG IN METHODS (OPTIONALLY AVAILABLE FEATURE) 2-2
CHAPTER 3 INSTALLATION 3-1
3.1 OVERVIEW 3-1
3.2 CATTRAX WEB INACTIVITY TIMEOUT FUNCTIONS 3-1
3.3 CATTRAX WEB INSTALLATION STEPS FOR MICROSOFT WINDOWS 10 3-2
3.3.1 Install Cattrax Web Application (Windows 10) 3-2
3.3.2 Custom Directory (Windows 10) 3-4
3.3.3 Setting the IIS Recycling Time and Idle Timeout (Windows 10) 3-4
3.3.4 Configure Windows Firewall (Windows 10) 3-5
3.3.5 Configuring IIS to Use LDAP (Windows 10) 3-5
3.3.6 Configure IIS for Secure Connections (Windows 10) 3-6
3.3.7 Test Cattrax Web Operation 3-6
3.4 CATTRAX WEB INSTALLATION STEPS FOR MICROSOFT WINDOWS 7 3-6
3.4.1 Install Cattrax Web Application (Windows 7) 3-7
3.4.2 Custom Directory (Windows 7) 3-8
3.4.3 Setting the IIS Recycling Time and Idle Timeout (Windows 7) 3-8
3.4.4 Configure Windows Firewall (Windows 7) 3-9
3.4.5 Configuring IIS to Use LDAP (Windows 7) 3-10
3.4.6 Configure IIS for Secure Connections (Windows 7) 3-10
3.4.7 Test Cattrax Web Operation 3-11
3.5 CATTRAX WEB INSTALLATION STEPS FOR MICROSOFT WINDOWS SERVER 2008. 3-11
3.5.1 Install Cattrax Web Application (Windows Server 2008) 3-11
3.5.2 Custom Directory (Windows Server 2008) 3-12
3.5.3 Setting the IIS Recycling Time and Idle Timeout (Windows Server 2008) 3-13
3.5.4 Configure Windows Firewall (Windows Server 2008) 3-13
3.5.5 Configuring IIS to Use LDAP (Windows Server 2008) 3-14
3.5.6 Configure IIS for Secure Connections (Windows Server 2008) 3-14
3.5.7 Test Cattrax Web Operation 3-15
3.6 CATTRAX WEB INSTALLATION STEPS FOR MICROSOFT WINDOWS SERVER 2012 AND SERVER 2012 R2 3-15
3.6.1 Install Cattrax Web Application (Windows Server 2012 and Server 2012 R2) 3-15
3.6.2 Custom Directory (Windows Server 2012 and Server 2012 R2) 3-18
3.6.3 Setting the IIS Recycling Time and Idle Timeout (Windows Server 2012 and Server 2012 R2) 3-18
3.6.4 Configure Windows Firewall (Windows Server 2012 and Server 2012 R2) 3-19
3.6.5 Configuring IIS to Use LDAP (Windows Server 2012 and Server 2012 R2) 3-19
3.6.6 Configure IIS for Secure Connections (Windows Server 2012 and Server 2012 R2) 3-20
3.6.7 Test Cattrax Web Operation 3-20

TABLE OF CONTENTS (CONT.)

3.7 CATTRAX WEB INSTALLATION STEPS FOR MICROSOFT WINDOWS SERVER 2016. 3-20
3.7.1 Install Cattrax Web Application (Windows Server 2016) 3-21
3.7.2 Custom Directory (Windows Server 2016) 3-23
3.7.3 Setting the IIS Recycling Time and Idle Timeout (Windows Server 2016) 3-24
3.7.4 Configure Windows Firewall (Windows Server 2016) 3-24
3.7.5 Configuring IIS to Use LDAP (Windows Server 2016) 3-25
3.7.6 Configure IIS for Secure Connections (Windows Server 2016) 3-25
3.7.7 Test Cattrax Web Operation 3-26
3.8 HOW TO MOVE A CATTRAX WEB DATABASE FROM A COMPUTER WITH SQL SERVER 2008R2 (WINDOWS XP/7/10) TO A COMPUTER WITH SQL SERVER 2014 (WINDOWS SERVER 2012 AND LATER). 3-26
3.9 TESTING CATTRAX WEB INSTALLATION 3-27
3.10 CONFIGURING THE FIREFOX BROWSER TO USE LDAP 3-27
3.11 CATTRAX WEB APPLICATION – UNINSTALL 3-28
CHAPTER 4 INITIAL LOGIN AND SETUP 4-1
4.1 INITIAL LOGIN AND LICENSE ACTIVATION 4-1
4.2 ACTIVATE SOFTWARE LICENSE KEY 4-1
4.2.1 Online Activation 4-2
4.2.2 Manual (Offline) Activation 4-3
4.3 CHANGE THE PASSWORD AND SECURITY QUESTION OF THE ADMIN USER ACCOUNT 4-4
4.4 CREATE A NEW USER ACCOUNT WITH ADMINISTRATOR PRIVILEGE 4-6
CHAPTER 5 OPERATION 5-1
5.1 INTRODUCTION 5-1
5.2 LOGIN TO CATTRAX WEB 5-2
5.3 LANDING PAGE 5-2
5.4 SETUP HOME PAGE 5-3
5.5 CONFIGURE DEVICE NETWORK (ADMINISTRATOR LEVEL USER) 5-4
5.6 OVERVIEW OF ADMINISTRATIVE FUNCTIONS 5-5
5.7 USER CONFIGURATION 5-6
5.7.1 User List Page 5-6
5.7.2 User Profile Page 5-11
5.7.3 User Groups 5-12
5.8 CATTRAX WEB CONTROL SYSTEM ARCHITECTURE OVERVIEW 5-14
5.9 CATTRAX WEB SYSTEM CONFIGURATION 5-15
5.10 HARDWARE CONFIGURATION PAGES 5-16
5.10.1 Controllers Page 5-16
5.10.2 Virtual Controllers Page 5-17
5.10.3 Create System Resource Include Lists 5-18
5.10.4 Subsystems 5-22

TABLE OF CONTENTS (CONT.)

5.11 WORKSPACES CONFIGURATION 5-24
5.12 SERVER CONFIGURATION FUNCTIONS 5-26
5.13 SERVER CONFIGURATION USER INTERFACE PAGE 5-27
5.13.1 Subnet Broadcast Address Configuration (Subnet Information) 5-28
5.13.2 System resource Icons (Display Options) 5-28
5.13.3 Switching or Routing Display Preference (Display Options) 5-28
5.13.4 System Broadcast Announcement Configuration (Display Options) 5-28
5.13.5 Custom Logo Configuration (Display options) 5-28
5.13.6 General Settings 5-29
5.13.7 Contact Information on Login Page 5-29
5.13.8 Administrative Email Communication Setup 5-29
5.13.9 User Inactivity Timer Configuration (Security Settings) 5-29
5.13.10 Login Dialog Box User Prompt Configuration (Security Settings) 5-30
5.13.11 Alternative Login Configuration (Active Directory & LDAP) 5-30
5.13.12 Error Mode (Error Messages Mode) 5-30
5.14 ALTERNATIVE LOG-IN CONFIGURATION (OPTIONALLY AVAILABLE FEATURE) ... 5-30
5.15 BACKUP & RESTORE 5-32
5.16 LICENSE 5-32
5.17 LOGS 5-32
5.18 SWITCHING PAGE 5-35
5.19 MENU BAR 5-36
5.20 WORKSPACE HEADER 5-37
5.21 SWITCHING AREA 5-37
5.21.1 Performing a Switch on the Router 5-37
5.21.2 Destination Lock Modes 5-38
5.21.3 Favorite Destinations 5-39
5.21.4 Undo Function 5-39
5.22 SALVOS WINDOW 5-39
5.23 SALVO CONFIGURATION (CREATE AND EDIT SALVO PAGE) 5-40
5.24 LOG DISPLAY 5-42
CHAPTER 6 EVENT SCHEDULING OPTION 6-1
6.1 INTRODUCTION 6-1
6.2 OVERVIEW 6-1
6.3 EVENT STACK PAGE 6-2
6.3.1 Event Stack Display Matrix 6-2
6.3.2 Master Event Scheduling Pause 6-4
6.4 SCHEDULE EDITING PAGE 6-4
6.5 CREATING SCHEDULE ITEMS 6-6
CHAPTER 7 IN THE EVENT OF DIFFICULTY 7-1
7.1 PESA CUSTOMER SERVICE 7-1

LIST OF FIGURES

FIGURE 2-1 EXAMPLE CATTRAX WEB USER INTERFACE PAGE 2-1

FIGURE 4-1 CATTRAX WEB LOGIN PAGE 4-1
FIGURE 4-2 LICENSE ACTIVATION PAGE 4-2
FIGURE 4-3 CATTRAX WEB SETUP HOME PAGE 4-4
FIGURE 4-4 USER PROFILE PAGE 4-5
FIGURE 4-5 USER LIST PAGE 4-6

FIGURE 5-1 CATTRAX WEB LOGIN PAGE 5-2
FIGURE 5-2 SETUP HOME PAGE 5-3
FIGURE 5-3 SERVER CONFIGURATION PAGE 5-4
FIGURE 5-4 TABLE DISPLAY FORMAT 5-6
FIGURE 5-5 USER LIST PAGE 5-6
FIGURE 5-6 USER PROFILE PAGE 5-11
FIGURE 5-7 USER GROUPS PAGE 5-13
FIGURE 5-8 CATTRAX WEB SYSTEM DIAGRAM 5-15
FIGURE 5-9 CONTROLLERS PAGE 5-16
FIGURE 5-10 VIRTUAL CONTROLLERS PAGE 5-17
FIGURE 5-11 CREATE LISTS PAGE 5-19
FIGURE 5-12 CREATE LISTS CONFIGURATION 5-20
FIGURE 5-13 SUBSYSTEMS PAGE 5-22
FIGURE 5-14 WORKSPACES PAGE 5-24
FIGURE 5-15 SERVER CONFIGURATION FUNCTIONS AND USER INTERFACE PAGE 5-27
FIGURE 5-16 BACKUP AND RESTORE PAGE 5-32
FIGURE 5-17 LOGS PAGE 5-33
FIGURE 5-18 EXAMPLE SWITCHING PAGE 5-35
FIGURE 5-19 SALVO EDIT PAGE 5-40

FIGURE 6-1 EXAMPLE EVENT STACK PAGE 6-3
FIGURE 6-2 EXAMPLE SCHEDULE EDITING PAGE 6-5
FIGURE 6-3 EXAMPLE SCHEDULE ITEM CREATION BOX 6-7

Chapter 1 About This Manual

1.1 Documentation and Safety Overview

This User Guide provides instructions for installation and operation of the Cattrax Web System Control Application, designed and produced by PESA.

It is the responsibility of all personnel involved in the installation, operation, and maintenance of the equipment to know all the applicable safety regulations for the areas they will be working in. ***Under no circumstances should any person perform any procedure or sequence in this manual if the procedural sequence will directly conflict with local Safe Practices. Local Safe Practices shall remain as the sole determining factor for performing any procedure or sequence outlined in this document.***

1.2 Cautions, and Notes

Cautions and Notes are addendum statements used in this guide that supply necessary information pertaining to the text or topic they address. Caution statements typically notify you of steps or procedures that could impede installation or operation; and/or cause damage to the equipment. Notes are additional statements that typically provide added information that can simplify and/or enhance the use or operating characteristics of the equipment. Examples of the graphic symbol used to identify each type of statement and the nature of the statement content are shown below:

	**Caution statements identify conditions or practices that can result in personal injury and/or damage to equipment if the instructions contained in the statement are not complied with.**

	**Notes are for information purposes only. However, they may contain invaluable information important to the correct installation, operation, and/or maintenance of the equipment.**

Chapter 2 Introduction

2.1 DESCRIPTION

PESA's Cattrax Web is a web application for use with the Microsoft Windows 10, Windows 7, Windows Server 2003, Windows Server 2008, Windows Server 2012 or Windows Server 2016 Operating System that allows users to monitor and control a wide variety of PESA routers from virtually any computer with TCP/IP network or internet access to the host server.

User access to Cattrax Web is through a common web browser application, such as Mozilla Firefox or Google Chrome. Cattrax Web communicates through the Ethernet interface of the user's PC directly with a PERC2000 or PERC3000 System Controller and performs in many respects as a PESA hardware remote control panel.

User interface with the application is through very intuitive pages and menus. An example Cattrax Web user interface page for switching functions is shown in Figure 2-1.

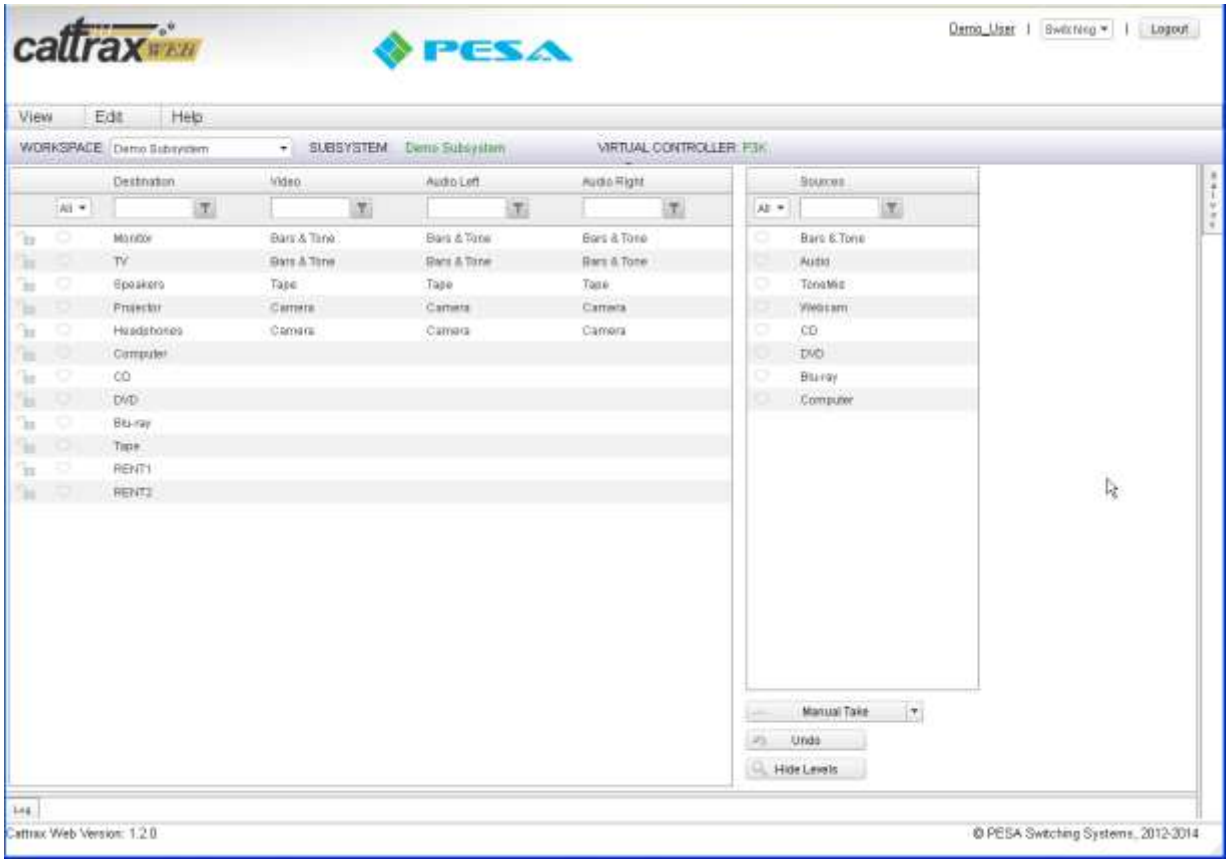


Figure 2-1 Example Cattrax Web User Interface Page

Access to the Cattrax Web system and router switching operations may be controlled by assigning users to any one of three user privilege levels:

- **Administrator** – Administrator level users are granted access to all pages and functions of Cattrax Web.

- **Supervisor** – Supervisor level users are granted access to both the Switching and Setup functional areas of Cattrax Web, with the exception of the server configuration pages. Following hierarchy, a Supervisor level user cannot:
  - Create a new Administrator level user account,
  - Grant Administrator level access to a new or existing user account, or
  - Edit the account or change access privilege of any user with Administrator privilege.
- **Staff** – Staff level users are granted access to only the Switching user interface pages and functions. When a Staff level user logs in to Cattrax Web the application opens immediately to the Switching page.

This User Guide assumes that administrative users who will be configuring the Cattrax Web application have knowledge of PESA router operation and system architecture, the router system controller device and the Cattrax system control software application. Administrative users should be familiar with creating and using controller configuration files, and PESA hardware remote control panel configuration and operation.

User Guides for all of these requisites are available on the Product Information CD included with your system or the PESA website at www.pesa.com.

Regardless of privilege level, all authorized users access router control through the **Switching (Routing)** operational area of Cattrax Web. The Switching (Routing) page identifies one or more ***workspace*** instances to which the specific logged-in user has been granted access. Workspace instances are created by system administrators or supervisors to very specifically assign and control router access to individual users or user groups.

2.2 ALTERNATE LOG IN METHODS (OPTIONALLY AVAILABLE FEATURE)

If this optional feature is licensed for your installation, Cattrax Web supports user log in with externally authenticated domain login credentials through either Microsoft Active Directory Domain Services (Active Directory) or a domain server running the Lightweight Directory Access Protocol (LDAP), if either, or both, of these network services are available on your facility's IT infrastructure.

Active Directory typically provides quicker access to the application by allowing an authorized user to automatically launch Cattrax Web using Windows domain login credentials instead of entering a Cattrax Web specific user ID and password.

Alternate log in methods can also provide additional user access security. Cattrax Web allows the system administrator to, for specified users, disable the Login Page option of entering application-specific user ID and password credentials assigned to the user at the time of account creation or through subsequent user account changes to access Cattrax Web, and allow these users access only by using authenticated domain login credentials.

These features can provide the system designer or security officer a great deal of latitude in controlling user access by effectively allowing the system administrator to assign, on an individual user basis, authorized methods of login access to Cattrax Web. For example, login access may be restricted for certain users in such a way to require use of a Common Access Card (CAC) card, a Personal Identity Verification (PIV) card, or other externally authenticated login credentials.

Alternate login privileges may be individually assigned to Cattrax Web users on an as-needed basis.

In order to use either of these methods, you must first configure Cattrax Web through settings entered on the Server Configuration page of the application during system set-up. Refer to paragraph 5.14.

Chapter 3 Installation

3.1 OVERVIEW

Preparing Cattrax Web for operation requires installation of the following main programs:

1. **Microsoft SQL Server Express** (or SQLExpress) – installed using the *Cattrax Web Prerequisites Setup.exe* program.

   NOTE: Ensure that there are no Microsoft SQL Server databases or SQL Server versions, other than for Cattrax Web, installed on the PC or server on which you are installing the application.

2. **Microsoft IIS** (Internet Information Services) – installed from the Windows Control Panel using procedures presented in the following paragraphs.

3. **Cattrax Web Application** – installed using the *Cattrax Web x.x.x Setup.exe* program. It includes any updates to the Cattrax Web database.

Microsoft Windows Operating System versions currently supported are Windows 10, Windows 7, Windows Server 2003, Windows Server 2008, Windows Server 2012 and Windows Server 2016. This document provides Cattrax Web installation steps for each operating system and includes additional detail information as required.

Install Cattrax Web for your particular operating system using procedures presented in paragraphs 3.3 thru 3.7.

While not a part of the initial installation procedure, for system planning purposes the installer should be aware that as an optionally available feature, Cattrax Web permits versatile user log in capabilities through the optional use of the Windows Active Directory Domain Services (Active Directory) or the Lightweight Directory Access Protocol (LDAP). The installer has the option of configuring user login access through either or both of these methods. The Cattrax Web application must be installed and operating before either of these login methods can be configured and implemented. Refer to Paragraph 2.2 for more information.

PESA recommends that you read this document and familiarize yourself with the Cattrax Web application and the procedures applicable to your operating system before starting the installation.

3.2 CATTRAX WEB INACTIVITY TIMEOUT FUNCTIONS

Microsoft IIS incorporates timeout functions that cause certain tasks to be executed after a set amount of time has elapsed. Cattrax Web makes use of this capability in two ways.

One is the user inactivity timeout, or *session timeout*, that causes IIS to drop a user's open session after a user has not had any active interface with the software application for a set amount of time. The amount of time for session timeout can be set by an administrative user from the Server Configuration page.

The second function is the *application idle timeout*. With this timeout when no user activity is detected for the set period of time, the Cattrax Web application is dropped by the server, communication is dropped between Cattrax Web and all discovered network devices, and all user pages, such as Switching pages, are closed. The purpose of having this capability is to reduce resource requirement of the server computer when the Cattrax Web application is not in use.

When a user logs in to Cattrax Web after an application idle timeout has occurred, the application must restart and reload all previous session data and reestablish communications with network devices. While it only takes a couple of minutes to restart the application, it is often desirable to have this time set to a value that would prevent an application timeout from occurring during what would be a normal workday or system use session.

The amount of time that must elapse before an application idle timeout occurs may be defined, but is not a setting that is available from the configuration pages. This value must be entered directly through the IIS Manager Utility.

Specific procedures for setting the application timeout with each supported operating system are provided in the following installation paragraphs.

3.3 CATTRAX WEB INSTALLATION STEPS FOR MICROSOFT WINDOWS 10

	**An active connection to the internet may be required for completion of the installation steps in the following paragraphs. If the PC or server device on which you are installing Cattrax Web will be used in a facility where internet access is not available, PESA recommends that you complete and test installation of the software before installing the device in the secure area.**

3.3.1 INSTALL CATTRAX WEB APPLICATION (WINDOWS 10)

1. Login with Administrator privilege to the server on which you wish to install Cattrax Web.
2. Insert the installation disk.
3. Run *Cattrax Web Prerequisites Setup.exe*, click *Next* when prompted. On the *Choose Components* page, leave all boxes checked unless instructed otherwise by PESA Customer Service. Select *Install* to continue with installation.

   While running the Prerequisites installation disk, if the installer application requests a restart of the computer, follow these guidelines:

   - Respond "Yes" to allow the computer to reboot if the installer asks permission.
   - Run the *Cattrax Web Prerequisites Setup.exe* file again after any reboots. This ensures all prerequisites are installed.

4. Click *"Finish"* to complete installation of Prerequisites.
5. Click *Start, Settings, Apps, Programs & Features, Turn Windows Features on or off.*

   Note: If your Windows 10 installation does not display the option "Turn Windows Features on or off", it could be hidden by an IT Group Policy restriction, even if your operator's account has Admin level privileges. If hidden, go to the Start → Run box and type "*appwiz.cpl*". This will display the dialog containing the "Turn Windows Features on or off" prompt.

6. Check the box next to *Internet Information Services*, and then expand it.
7. Expand *World Wide Web Services*, and then expand *Application Development Services*.
8. Check the box next to *ASP.NET 3.5*.
9. Expand the *Common HTTP Features* entry from the tree.

10. Place a check in the box beside *HTTP Errors* and *Static Content*.
11. If you will be using the *Additional Login Options* feature, follow the next two steps; otherwise, skip to Step 14.
12. Expand the *Security* entry from the tree.
13. Check the box next to *Windows Authentication*.
14. Click *Ok*.
15. Run *Cattrax Web x.x.x Setup.exe*, click *Next* at the initial prompt. You will be asked to read and agree to the terms of the Cattrax Web software license. Click *"I Agree"* to continue with installation.
16. On the *Choose Components* page, leave all three boxes checked unless instructed otherwise by PESA Customer Service. Click *"Next"* to continue to the *"Choose Installation Location"* prompt.
17. Use of the default install location is recommended; however, you may change the default location in the "Choose Install Location" page of the wizard. Be aware, that choosing a location that is outside the wwwroot directory might interfere with access to the Cattrax Web website. Click *"Install"* to begin the installation process.

    Note: If a **Database Update Error** popup message is displayed, click OK. Repeat steps 15 and 16. It may be necessary to repeat steps 15 and 16 up to three (3) times in order to resolve all database update errors.

18. A progress bar allows you verify installation. If a popup is displayed asking permission to shutdown Cattrax Web, click OK. Upon completion, you will be prompted to click *"Finish"* to complete the installation process.
19. Under Administrative Tools, start Internet Information Services (IIS)
20. In the left panel, expand *Sites*.
21. Double click *Sites -> Default Web Site.*
22. Double click the *CSS* directory.
23. Right click the *Images* directory and select *"Edit Permissions…"*.
24. Select the *Security* tab.
25. Click *Edit.*
26. Select *ASP.NET Machine Account*. If that entry is not listed, select *"IIS_USERS"*.
27. Click the *Write* check box in the *Allow* column.
28. Click OK to close the *Edit* dialog.
29. Click OK to close the *Properties* dialog.

On 64-bit systems, you will need to configure IIS to run 32-bit applications, as follows:

1. Under Administrative Tools, start Internet Information Services (IIS).
2. Expand the first node on the *Connections* panel and click *Application Pools*.
3. Right-click *DefaultAppPool*, select Advanced Settings, and change *Enable 32-Bit Applications* to *True*, if that option is not already selected.
4. Click OK.

3.3.2 CUSTOM DIRECTORY (WINDOWS 10)

The default installation directory is: c:\InetPub\wwwroot. **Use of this directory is recommended**.

A custom installation directory may also be selected. For example: c:\MySites\CattraxWeb. This should be used if another website is already installed in the root directory.

After changing the default directory, configure a virtual directory as follows:

1. Under Administrative Tools, start Internet Information Services (IIS).
2. Expand Web Sites and then right click Default Web Site.
3. Click "Add Application…".
4. On the Add Application window, in field labeled Alias, enter a name to follow the host address (i.e. if the Alias is named CattraxWeb, the address would be 192.168.1.1/CattraxWeb).
5. In the field labeled Physical Path, enter the path to the directory where the Cattrax Web wwwroot directory was installed. (i.e. if the custom directory is named cw, then the path would be C:\inetpub\wwwroot\cw\wwwroot).
6. Click OK.
7. Test the installation by opening a browser and typing localhost/[Alias].

3.3.3 SETTING THE IIS RECYCLING TIME AND IDLE TIMEOUT (WINDOWS 10)

In order to set the IIS recycling time through Windows 10 use the following procedure:

1. Under Administrative Tools, start Internet Information Services (IIS).
2. On the left side of the window under "Connections", expand the local computer name.
3. Click the *Application Pools* entry.
4. In the middle panel, Application Pools, select the *DefaultAppPool* entry.
5. In the right panel, select the *Set Application Pool Defaults* entry.
6. In the dialog under Process Model, edit the Idle Time-out. Enter a value such as 480 minutes.

   NOTE: The "minutes" value entered will set the amount of time during which the CattraxWeb application will not be unloaded by IIS should no user command be received, such as changing which page is displayed, entering data, or making a switch. Using the example of 480 minutes will set the Idle Time-out at 8 hours.
7. Scroll down to the *Recycling* entry.
8. Under *Regular Time Interval*, set the value to zero (0).
9. Click the "…" item in the right side of the *Specific Times* entry.
10. Click *Add* in the dialog.
11. Enter a specific time of day, such as 01:00:00 for 1 AM. Select a time of day which is low demand.
12. Click *OK* to accept the time value entered.
13 Click *OK* to close the dialog.
14. Restart IIS to activate settings.

3.3.4 CONFIGURE WINDOWS FIREWALL (WINDOWS 10)

Use this procedure if you are using the Windows Firewall in Windows 10 in the Cattrax Web host server:

1. Under *Administrative Tools*, run *Windows Firewall with Advanced Security*.
2. In the left panel, click *Inbound Rules*.
3. In the right panel, click *New Rule*.
4. In *Rule Type* window, select *Port* and click Next.
5. In the *Program* window, select *All Programs* and click Next.
6. In *Protocol and Ports*, select *TCP and Specified local ports*, and set the port value to 80 and click Next.
7. In *Action*, select *Allow the Connection* and click Next.
8. In *Profile*, select all items (or as appropriate based on who would have access to Cattrax Web) and click Next.
9. In *Name*, give this rule a name and optionally a description and click on Finish. A good name to use is "HTTP".
10. Repeat steps 1 thru 9 above using a port value of 443 and the name "HTTPS".

NOTE	It is also possible to turn off the firewall completely but **NOT RECOMMENDED.**

3.3.5 CONFIGURING IIS TO USE LDAP (WINDOWS 10)

1. Under Administrative Tools, start Internet Information Services (IIS).
2. In the left panel, select Sites -> Default Web Site.
3. In the middle panel, open Authentication under Security.
4. Set Windows Authentication to Disabled.
5. If Forms Authentication is listed, set it to Disabled.
6. If Anonymous Authentication is listed, set it to Enabled.
7. In the left panel, select Sites -> Default Web Site -> NTLM.
8. In the middle panel, open Authentication under Security.
9. Set Windows Authentication to Enabled.
10. If Forms Authentication is listed, set it to Disabled.
11. If Anonymous Authentication is listed, set it to Disabled.
12. Exit IIS Manager.

3.3.6 CONFIGURE IIS FOR SECURE CONNECTIONS (WINDOWS 10)

By default, IIS accepts only non-secure connections (http protocol). IIS can be configured to accept secure connections (https protocol) using Secure Sockets Layer (SSL) in addition to non-secure connections. IIS can also be configured to accept only secure connections.

In addition to configuration IIS, the web server will also need a certificate. If you do not have a certificate, one will need to be created. You can either create a self-signed certificate or obtain a certificate from a recognized Certificate Authority (CA). For information on how to create a self-signed certificate, go to http://msdn.microsoft.com/en-us/library/bfsktky3(v=vs.90).aspx. For information about how to obtain a certificate from a recognized Certificate Authority (CA), contact your administrator.

Configure Windows 10 IIS to Accept Secure Connections as follows:

1. Under Administrative Tools, start Internet Information Services (IIS).
2. Select the Cattrax Web website in the left panel. Unless a custom directory was selected during the installation, it will be "Default Web Site".
3. Right click on the tree node and select "Edit Bindings".
4. Click the "Add..." button.
5. Select "https" in the "Type:" drop-down list.
6. Select your SSL certificate in the "SSL certificate:" drop-down list.
7. Leave the other values text boxes unchanged unless given different values by your administrator.
8. Click the "OK" button to close the "Add Site Binding" dialog box.
9. Click the "Close" button to close the "Site Bindings" dialog box.

To also disable non-secure connections, continue with these steps:

10. Ensure the website node is still selected in the left panel.
11. Double click the "SSL Settings" item.
12. Check the "Require SSL" checkbox.

For more information on enabling secure connections in Windows 10, refer to
http://www.iis.net/learn/manage/configuring-security/how-to-set-up-ssl-on-iis

3.3.7 TEST CATTRAX WEB OPERATION

Upon completion of installation, test Cattrax Web operation in accordance with paragraph 3.9.

3.4 CATTRAX WEB INSTALLATION STEPS FOR MICROSOFT WINDOWS 7

NOTE	**An active connection to the internet may be required for completion of the installation steps in the following paragraphs. If the PC or server device on which you are installing Cattrax Web will be used in a facility where internet access is not available, PESA recommends that you complete and test installation of the software before installing the device in the secure area.**

3.4.1 INSTALL CATTRAX WEB APPLICATION (WINDOWS 7)

1. Login with Administrator privilege to the server on which you wish to install Cattrax Web.
2. Insert the installation disk.
3. Run *Cattrax Web Prerequisites Setup.exe*, click *Next* when prompted. On the *Choose Components* page, leave all boxes checked unless instructed otherwise by PESA Customer Service. Select *Install* to continue with installation.

   While running the Prerequisites installation disk, if the installer application requests a restart of the computer, follow these guidelines:

   - Respond "Yes" to allow the computer to reboot if the installer asks permission.
   - Run the *Cattrax Web Prerequisites Setup.exe* file again after any reboots. This ensures all prerequisites are installed.

4. Click *"Finish"* to complete installation of Prerequisites.
5. Click *Start, Control Panel, Programs, Turn Windows Features on or off*.
6. Check the box next to *Internet Information Services*, and then expand it.
7. Expand *World Wide Web Services*, and then expand *Application Development Features*.
8. Check the box next to *ASP.NET*.
9. Expand the *Common HTTP Features* entry from the tree.
10. Place a check in the box beside *HTTP Errors* and *Static Content*.
11. If you will be using the *Additional Login Options* feature, follow the next two steps; otherwise, skip to Step 14.
12. Expand the *Security* entry from the tree.
13. Check the box next to *Windows Authentication*.
14. Click *Ok*.
15. Run *Cattrax Web x.x.x Setup.exe*, click *Next* at the initial prompt. You will be asked to read and agree to the terms of the Cattrax Web software license. Click *"I Agree"* to continue with installation.
16. On the *Choose Components* page, leave all three boxes checked unless instructed otherwise by PESA Customer Service. Click *"Next"* to continue to the *"Choose Installation Location"* prompt.
17. Use of the default install location is recommended; however, you may change the default location in the "Choose Install Location" page of the wizard. Be aware, that choosing a location that is outside the wwwroot directory might interfere with access to the Cattrax Web website. Click *"Install"* to begin the installation process.

    Note: If a **Database Update Error** popup message is displayed, click OK. Repeat steps 15 and 16. It may be necessary to repeat steps 15 and 16 up to three (3) times in order to resolve all database update errors.

18. A progress bar allows you verify installation. Upon completion, you will be prompted to click *"Finish"* to complete the installation process.
19. Under Administrative Tools, start Internet Information Services (IIS).

20. In the left panel, expand *Sites*.
21. Double click *Sites -> Default Web Site.*
22. Double click the *CSS* directory.
23. Right click the *Images* directory and select *"Edit Permissions…"*.
24. Select the *Security* tab.
25. Click *Edit.*
26. Select *ASP.NET Machine Account*. If that entry is not listed, select *"IIS_USERS"*.
27. Click the *Write* check box in the *Allow* column.
28. Click OK to close the *Edit* dialog.
29. Click OK to close the *Properties* dialog.

On 64-bit systems, you will need to configure IIS to run 32-bit applications, as follows:

1. Under Administrative Tools, start Internet Information Services (IIS).
2. Expand the first node on the *Connections* panel and click *Application Pools*.
3. Right-click *DefaultAppPool*, select Advanced Settings, and change *Enable 32-Bit Applications* to *True*, if that option is not already selected.
4. Click OK.

3.4.2 CUSTOM DIRECTORY (WINDOWS 7)

The default installation directory is: c:\InetPub\wwwroot. **Use of this directory is recommended**.

A custom installation directory may also be selected. For example: c:\MySites\CattraxWeb. This should be used if another website is already installed in the root directory.

After changing the default directory, configure a virtual directory as follows:

1. Under Administrative Tools, start Internet Information Services (IIS).
2. Expand Web Sites and then right click Default Web Site.
3. Click "Add Application…".
4. On the Add Application window, in field labeled Alias, enter a name to follow the host address (i.e. if the Alias is named CattraxWeb, the address would be 192.168.1.1/CattraxWeb).
5. In the field labeled Physical Path, enter the path to the directory where the Cattrax Web wwwroot directory was installed. (i.e. if the custom directory is named cw, then the path would be C:\inetpub\wwwroot\cw\wwwroot).
6. Click OK.
7. Test the installation by opening a browser and typing localhost/[Alias].

3.4.3 SETTING THE IIS RECYCLING TIME AND IDLE TIMEOUT (WINDOWS 7)

In order to set the IIS recycling time through Windows 7 use the following procedure:

1. Under Administrative Tools, start Internet Information Services (IIS).
2. On the left side of the window under "Connections", expand the local computer name.

3. Click the *Application Pools* entry.
4. In the middle panel, Application Pools, select the *DefaultAppPool* entry.
5. In the right panel, select the *Set Application Pool Defaults* entry.
6. In the dialog under Process Model, edit the Idle Time-out. Enter a value such as 480 minutes.

   NOTE: The "minutes" value entered will set the amount of time during which the CattraxWeb application will not be unloaded by IIS if no user command is received, such as changing which page is displayed, entering data, or making a switch. Using the example of 480 minutes will set the Idle Time-out at 8 hours.
7. Scroll down to the *Recycling* entry.
8. Under *Regular Time Interval*, set the value to zero (0).
9. Click the "…" item in the right side of the *Specific Times* entry.
10. Click *Add* in the dialog.
11. Enter a specific time of day, such as 01:00:00 for 1 AM. Select a time of day which is low demand.
12. Click *OK* to accept the time value entered.
13 Click *OK* to close the dialog.
14. Restart IIS to activate settings.

3.4.4 CONFIGURE WINDOWS FIREWALL (WINDOWS 7)

Use this procedure if you are using the Windows Firewall in Windows 7 in the Cattrax Web host server:

1. Open - Control Panel from the Start menu.
2. Open - Windows Firewall.
3. From the left column, open Advanced Settings.
4. Select New Rules from the Inbound Rules right click menu in the left column and then follow the wizard as follows:
   a. In Rule Type window – select Port and click *Next,*
   b. In Protocol and Ports – Select TCP and Specified local ports, and set the port value to 80 and click *Next,*
   c. In Action window – Select Allow the Connection and click *Next,*
   d. In Profile window – Select all items (or as appropriate based on who would have access to Cattrax Web) and click *Next,*
   e. In the Name window – Give this special set up a name and description and click on Finish. A good name to use for such a special setup would be "HTTP".

NOTE	It is also possible to turn off the firewall completely but **NOT RECOMMENDED.**

3.4.5 CONFIGURING IIS TO USE LDAP (WINDOWS 7)

1. Under Administrative Tools, start Internet Information Services (IIS).
2. In the left panel, select Sites -> Default Web Site.
3. In the middle panel, open Authentication under Security.
4. Set Windows Authentication to Disabled.
5. If Forms Authentication is listed, set it to Disabled.
6. If Anonymous Authentication is listed, set it to Enabled.
7. In the left panel, select Sites -> Default Web Site -> NTLM.
8. In the middle panel, open Authentication under Security.
9. Set Windows Authentication to Enabled.
10. If Forms Authentication is listed, set it to Disabled.
11. If Anonymous Authentication is listed, set it to Disabled.
12. Exit IIS Manager.

3.4.6 CONFIGURE IIS FOR SECURE CONNECTIONS (WINDOWS 7)

By default, IIS accepts only non-secure connections (http protocol). IIS can be configured to accept secure connections (https protocol) using Secure Sockets Layer (SSL) in addition to non-secure connections. IIS can also be configured to accept only secure connections.

In addition to configuration IIS, the web server will also need a certificate. If you do not have a certificate, one will need to be created. You can either create a self-signed certificate or obtain a certificate from a recognized Certificate Authority (CA). For information on how to create a self-signed certificate, go to http://msdn.microsoft.com/en-us/library/bfsktky3(v=vs.90).aspx. For information about how to obtain a certificate from a recognized Certificate Authority (CA), contact your administrator.

Configure Windows 7 IIS to Accept Secure Connections as follows:

13. Under Administrative Tools, start Internet Information Services (IIS).
14. Select the Cattrax Web website in the left panel. Unless a custom directory was selected during the installation, it will be "Default Web Site".
15. Right click on the tree node and select "Edit Bindings".
16. Click the "Add..." button.
17. Select "https" in the "Type:" drop-down list.
18. Select your SSL certificate in the "SSL certificate:" drop-down list.
19. Leave the other values text boxes unchanged unless given different values by your administrator.
20. Click the "OK" button to close the "Add Site Binding" dialog box.
21. Click the "Close" button to close the "Site Bindings" dialog box.

To also disable non-secure connections, continue with these steps:

22. Ensure the website node is still selected in the left panel.

23. Double click the "SSL Settings" item.
24. Check the "Require SSL" checkbox.

For more information on enabling secure connections in Windows 7, refer to http://www.iis.net/learn/manage/configuring-security/how-to-set-up-ssl-on-iis.

3.4.7 TEST CATTRAX WEB OPERATION

Upon completion of installation, test Cattrax Web operation in accordance with paragraph 3.9.

3.5 CATTRAX WEB INSTALLATION STEPS FOR MICROSOFT WINDOWS SERVER 2008

NOTE	**An active connection to the internet may be required for completion of the installation steps in the following paragraphs. If the PC or server device on which you are installing Cattrax Web will be used in a facility where internet access is not available, PESA recommends that you complete and test installation of the software before installing the device in the secure area.**

3.5.1 INSTALL CATTRAX WEB APPLICATION (WINDOWS SERVER 2008)

1. Login with Administrator privilege to the server on which you wish to install Cattrax Web.
2. Insert the installation disk.
3. Run *Cattrax Web Prerequisites Setup.exe*, click *Next* when prompted. On the *Choose Components* page, leave all boxes checked unless instructed otherwise by PESA Customer Service. Select *Install* to continue with installation.

   While running the Prerequisites installation disk, if the installer application requests a restart of the computer, follow these guidelines:

   - Respond "Yes" to allow the computer to reboot if the installer asks permission.
   - Run the *Cattrax Web Prerequisites Setup.exe* file again after any reboots. This ensures all prerequisites are installed.

4. Click *"Finish"* to complete installation of Prerequisites.
5. Click Start, and then Server Manager.
6. On the left panel, click Roles, and then click Add Roles.
7. On Before You Begin, click Next.
8. On Select Server Roles, click Add Required Features, and then click Next.
9. On Web Server (IIS), click Next.
10. On Select Server Roles, check ASP.NET under Application Development, and then click Next.
11. On Confirmation, click Install.
12. On Confirm Installation Selections, click Install.
13. Run *Cattrax Web x.x.x Setup.exe*, click *Next* at the initial prompt. You will be asked to read and agree to the terms of the Cattrax Web software license. Click *"I Agree"* to continue with installation.

14. On the *Choose Components* page, leave all three boxes checked unless instructed otherwise by PESA Customer Service. Click *"Next"* to continue to the *"Choose Installation Location"* prompt.
15. Use of the default install location is recommended; however, you may change the default location in the "Choose Install Location" page of the wizard. Be aware, that choosing a location that is outside the wwwroot directory might interfere with access to the Cattrax Web website. Click *"Install"* to begin the installation process.

    Note: If a **Database Update Error** popup message is displayed, click OK. Repeat steps 13 and 14. It may be necessary to repeat steps 13 and 14 up to three (3) times in order to resolve all database update errors.

16. A progress bar allows you verify installation. Upon completion, you will be prompted to click *"Finish"* to complete the installation process.
17. Under Administrative Tools, start Internet Information Services (IIS).
18. In the left panel, expand *Sites*.
19. Double click *Sites -> Default Web Site.*
20. Double click the *CSS* directory.
21. Right click the *Images* directory and select *"Edit Permissions…"*.
22. Select the *Security* tab.
23. Click *Edit.*
24. Select *ASP.NET Machine Account*. If that entry is not listed, select *"IIS_USERS"*.
25. Click the *Write* check box in the *Allow* column.
26. Click OK to close the *Edit* dialog.
27. Click OK to close the *Properties* dialog.

On 64-bit systems, you will need to configure IIS to run 32-bit applications, as follows:

1. Under Administrative Tools, start Internet Information Services (IIS).
2. Expand the first node on the *Connections* panel and click *Application Pools*.
3. Right-click *DefaultAppPool*, select Advanced Settings, and change *Enable 32-Bit Applications* to *True*, if that option is not already selected.
4. Click OK.

3.5.2 CUSTOM DIRECTORY (WINDOWS SERVER 2008)

The default installation directory is: c:\InetPub\wwwroot. **Use of this directory is recommended**.

A custom installation directory may also be selected. For example: c:\MySites\CattraxWeb. This should be used if another website is already installed in the root directory.

After changing the default directory, configure a virtual directory as follows:

1. Under Administrative Tools, start Internet Information Services (IIS).
2. Expand Sites and then right click Default Web Site.
3. Click *New*, and then click "Add Application..".

4. On the Add Application window, in field labeled Alias, enter a name to follow the host address (i.e. if the Alias is named CattraxWeb, the address would be 192.168.1.1/CattraxWeb).
5. In the field labeled Physical Path, enter the path to the directory where the Cattrax Web wwwroot directory was installed. (i.e. if the custom directory is named cw, then the path would be C:\inetpub\wwwroot\cw\wwwroot).
6. Click OK.
7. Test the installation by opening a browser and typing localhost/[Alias].

3.5.3 SETTING THE IIS RECYCLING TIME AND IDLE TIMEOUT (WINDOWS SERVER 2008)

In order to set the IIS recycling time through Windows Server 2008 use the following procedure:

1. Under Administrative Tools, start Internet Information Services (IIS).
2. On the left side of the window under "Connections", expand the local computer name.
3. Click the *Application Pools* entry.
4. In the middle panel, Application Pools, select the *DefaultAppPool* entry.
5. In the right panel, select the *Set Application Pool Defaults* entry.
6. In the dialog under Process Model, edit the Idle Time-out. Enter a value such as 480 minutes.

   NOTE: The "minutes" value entered will set the amount of time during which the CattraxWeb application will not be unloaded by IIS if no user command is received, such as changing which page is displayed, entering data, or making a switch. Using the example of 480 minutes will set the Idle Time-out at 8 hours.
7. Scroll down to the *Recycling* entry.
8. Under *Regular Time Interval*, set the value to zero (0).
9. Click the "…" item in the right side of the *Specific Times* entry.
10. Click *Add* in the dialog.
11. Enter a specific time of day, such as 01:00:00 for 1 AM. Select a time of day which is low demand.
12. Click *OK* to accept the time value entered.
13 Click *OK* to close the dialog.
14. Restart IIS to activate settings.

3.5.4 CONFIGURE WINDOWS FIREWALL (WINDOWS SERVER 2008)

Use this procedure if you are using the Windows Firewall in Windows Server 2008 in the Cattrax Web host server:

1. Open - Control Panel from the Start menu.
2. Open - Windows Firewall.
3. From the left column, open Advanced Settings.

4. Select New Rules from the Inbound Rules right click menu in the left column and then follow the wizard as follows:
    a. In Rule Type window – select Port and click *Next*,
    b. In Protocol and Ports – Select TCP and Specified local ports, and set the port value to 80 and click *Next*,
    c. In Action window – Select Allow the Connection and click *Next*,
    d. In Profile window – Select all items (or as appropriate based on who would have access to Cattrax Web) and click *Next*,
    e. In the Name window – Give this special set up a name and description and click on Finish. A good name to use for such a special setup would be "HTTP".

NOTE	It is also possible to turn off the firewall completely but **NOT RECOMMENDED.**

3.5.5 CONFIGURING IIS TO USE LDAP (WINDOWS SERVER 2008)

1. Under Administrative Tools, start Internet Information Services (IIS).
2. In the left panel, select Sites -> Default Web Site.
3. In the middle panel, open Authentication under Security.
4. Set Windows Authentication to Disabled.
5. Set Forms Authentication to Disabled.
6. Set Anonymous Authentication to Enabled.
7. In the left panel, select Sites -> Default Web Site -> NTLM.
8. In the middle panel, open Authentication under Security.
9. Set Windows Authentication to Enabled.
10. Set Forms Authentication to Disabled.
11. Set Anonymous Authentication to Disabled.
12. Exit IIS Manager.

3.5.6 CONFIGURE IIS FOR SECURE CONNECTIONS (WINDOWS SERVER 2008)

By default, IIS accepts only non-secure connections (http protocol). IIS can be configured to accept secure connections (https protocol) using Secure Sockets Layer (SSL) in addition to non-secure connections. IIS can also be configured to accept only secure connections.

In addition to configuration IIS, the web server will also need a certificate. If you do not have a certificate, one will need to be created. You can either create a self-signed certificate or obtain a certificate from a recognized Certificate Authority (CA). For information on how to create a self-signed certificate, go to http://msdn.microsoft.com/en-us/library/bfsktky3(v=vs.90).aspx. For information about how to obtain a certificate from a recognized Certificate Authority (CA), contact your administrator.

Configure Windows Server 2008 IIS to Accept Secure Connections as follows:

1. Under Administrative Tools, start Internet Information Services (IIS).
2. Select the Cattrax Web website in the left panel. Unless a custom directory was selected during the installation, it will be "Default Web Site".
3. Right click on the tree node and select "Edit Bindings".
4. Click the "Add..." button.
5. Select "https" in the "Type:" drop-down list.
6. Select your SSL certificate in the "SSL certificate:" drop-down list.
7. Leave the other values text boxes unchanged unless given different values by your administrator.
8. Click the "OK" button to close the "Add Site Binding" dialog box.
9. Click the "Close" button to close the "Site Bindings" dialog box.

   To also disable non-secure connections, continue with these steps:

10. Ensure the website node is still selected in the left panel.
11. Double click the "SSL Settings" item.
12. Check the "Require SSL" checkbox.
13. For more information on enabling secure connections in Windows Server 2008, refer to http://www.iis.net/learn/manage/configuring-security/how-to-set-up-ssl-on-iis.

3.5.7 TEST CATTRAX WEB OPERATION

Upon completion of installation, test Cattrax Web operation in accordance with paragraph 3.9.

3.6 CATTRAX WEB INSTALLATION STEPS FOR MICROSOFT WINDOWS SERVER 2012 AND SERVER 2012 R2

	**An active connection to the internet may be required for completion of the installation steps in the following paragraphs. If the PC or server device on which you are installing Cattrax Web will be used in a facility where internet access is not available, PESA recommends that you complete and test installation of the software before installing the device in the secure area.**

3.6.1 INSTALL CATTRAX WEB APPLICATION (WINDOWS SERVER 2012 AND SERVER 2012 R2)

1. Login with Administrator privilege to the server on which you wish to install Cattrax Web.
2. Start the Server Manager.
3. Click Add Roles and Features.
4. On Before You Begin, click Next.
5. On Installation Type, select the correct choice for your system and click Next.
6. On Server Selection, select the correct choice for your system and click Next.

7. On Server Roles, select Web Server (IIS) -> Web Server -> Application Development ->.NET Extensibility 3.5.
8. If a Dialog appears asking permission to install .NET Framework 3.5, Check the box “Include management tools” and then click “Add Features”; otherwise, proceed to Step 9.
9. Select Web Server (IIS) -> Web Server -> Application Development -> ASP.NET 3.5.
10. Click Next.
11. On Features, select >NET Framework 3.5 Features -> .NET Framework 3.5.
12. On Features, select >NET Framework 3.5 Features -> .NET Framework 3.5 -> HTTP Activation.
13. If a Dialog appears asking permission to install .NET Environment 3.5, Check the box “Include management tools” and then click “Add Features”; otherwise, proceed to Step 14.
14. Select >NET Framework 4.x Features -> WCF Services.
15. Click Next.
16. On Confirmation, specify an alternate source path if necessary.
17. On confirmation, click Install.
18. When finished, click “Close”.
19. Exit Server Manager.
20. Under Administrative Tools, start Internet Information Services (IIS).
21. In the left panel, expand the local computer name.
22. Click the Application Pools entry.
23. In the middle panel, Application Pools, select the DefaultAppPool entry.
24. In the right panel under Edit Application Pool, click Advanced Settings.
25. In the dialog, ensure that General -> Enable 32-Bit Applications is set to True.
26. Scroll down to Recycling -> Specific Times.
27. Click the … item to the right of TimeSpan[] Array.
28. If a textbox is not displayed in the left column, click Add.
29. Enter a specific time of day, such as 01:00:00 for 1 AM in the field next to Value. Select a time of day which is low demand.
30. Click OK to accept the time value entered.
31. Click OK to close the Application Pool Defaults dialog.
32. In the left panel, select Sites -> Default Web Site.
33. In the right panel under Actions, click Basic Settings.
34. Ensure that “%SystemDrive%\inetpub\wwwroot “ or “C:\intepub\wwwroot” is in the text box Physical path.
35. Ensure that the Application Pool is set to DefaultAppPool.
36. Click OK to close the Edit Site dialog.
37. Exit IIS Manager.

38. Insert the Cattrax Web installation disk.
39. Run *Cattrax Web Prerequisites Setup.exe*, click *Next* when prompted. On the *Choose Components* page, leave all boxes checked unless instructed otherwise by PESA Customer Service. Select *Install* to continue with installation.

    While running the Prerequisites installation disk, if the installer application requests a restart of the computer, follow these guidelines:

    - Respond "Yes" to allow the computer to reboot if the installer asks permission.
    - Run the *Cattrax Web Prerequisites Setup.exe* file again after any reboots. This ensures all prerequisites are installed.
40. Click *"Finish"* to complete installation of Prerequisites.
41. Run *Cattrax Web x.x.x Setup.exe*, click *Next* at the initial prompt. You will be asked to read and agree to the terms of the Cattrax Web software license. Click *"I Agree"* to continue with installation.
42. On the *Choose Components* page, leave all three boxes checked unless instructed otherwise by PESA Customer Service. Click *"Next"* to continue to the *"Choose Installation Location"* prompt.
43. Use of the default install location is recommended; however, you may change the default location in the "Choose Install Location" page of the wizard. Be aware, that choosing a location that is outside the wwwroot directory might interfere with access to the Cattrax Web website. Click *"Install"* to begin the installation process.

    Note: If a **Database Update Error** popup message is displayed, click OK. Repeat steps 41 and 42. It may be necessary to repeat steps 41 and 42 up to three (3) times in order to resolve all database update errors.

44. A progress bar allows you verify installation. Upon completion, you will be prompted to click *"Finish"* to complete the installation process.
44. Under Administrative Tools, start Internet Information Services (IIS).
45. In the left panel, expand *Sites*.
46. Double click *Sites -> Default Web Site.*
47. Double click the *CSS* directory.
48. Right click the *Images* directory and select *"Edit Permissions…"*.
49. Select the *Security* tab.
50. Click *Edit.*
51. Select *ASP.NET Machine Account*. If that entry is not listed, select *"IIS_USERS"*.
52. Click the *Write* check box in the *Allow* column.
53. Click OK to close the *Edit* dialog.
54. Click OK to close the *Properties* dialog.

On 64-bit systems, you will need to configure IIS to run 32-bit applications, as follows:

1. Under Administrative Tools, start Internet Information Services (IIS).
2. Expand the first node on the *Connections* panel and click *Application Pools*.

3. Right-click *DefaultAppPool*, select Advanced Settings, and change *Enable 32-Bit Applications* to *True*, if that option is not already selected.
4. Click OK.

3.6.2 CUSTOM DIRECTORY (WINDOWS SERVER 2012 AND SERVER 2012 R2)

The default installation directory is: c:\InetPub\wwwroot. **Use of this directory is recommended**.

A custom installation directory may also be selected. For example: c:\MySites\CattraxWeb. This should be used if another website is already installed in the root directory.

After changing the default directory, configure a virtual directory as follows:

1. Under Administrative Tools, start Internet Information Services (IIS).
2. In the left panel, select Sites -> Default Web Site.
3. In the right panel under Actions, click Basic Settings.
4. Enter the path you want to use in the text box Physical path.
5. Click OK to close the Edit Site dialog.
6. Exit IIS Manager.

3.6.3 SETTING THE IIS RECYCLING TIME AND IDLE TIMEOUT (WINDOWS SERVER 2012 AND SERVER 2012 R2)

In order to set the recycling time through Windows Server 2012 and Server 2012 R2 use the following procedure:

1. Under Administrative Tools, start Internet Information Services (IIS).
2. On the left side of the window under "Connections", expand the local computer name.
3. Click the *Application Pools* entry.
4. In the middle panel, Application Pools, select the *DefaultAppPool* entry.
5. In the right panel, select the *Set Application Pool Defaults* entry.
6. In the dialog under Process Model, edit the Idle Time-out. Enter a value such as 480 minutes.

   NOTE: The "minutes" value entered will set the amount of time during which the CattraxWeb application will not be unloaded by IIS if no user command is received, such as changing which page is displayed, entering data, or making a switch. Using the example of 480 minutes will set the Idle Time-out at 8 hours.
7. Scroll down to the *Recycling* entry.
8. Under *Regular Time Interval*, set the value to zero (0).
9. Click the "…" item in the right side of the *Specific Times* entry.
10. Click *Add* in the dialog.
11. Enter a specific time of day, such as 01:00:00 for 1 AM. Select a time of day which is low demand.
12. Click *OK* to accept the time value entered.

13 Click *OK* to close the dialog.

14. Restart IIS to activate settings.

3.6.4 CONFIGURE WINDOWS FIREWALL (WINDOWS SERVER 2012 AND SERVER 2012 R2)

Use this procedure if you are using the Windows Firewall in Windows Server 2012 and Server 2012 R2 in the Cattrax Web host server:

1. Under *Administrative Tools*, run *Windows Firewall with Advanced Security*.
2. In the left panel, click *Inbound Rules.*
3. In the right panel, click *New Rule*.
4. In *Rule Type* window, select *Port* and click Next.
5. In the *Program* window, select *All Programs* and click Next.
6. In *Protocol and Ports*, select *TCP and Specified local ports*, and set the port value to 80 and click Next.
7. In *Action*, select *Allow the Connection* and click Next.
8. In *Profile*, select all items (or as appropriate based on who would have access to Cattrax Web) and click Next.
9. In *Name*, give this rule a name and optionally a description and click on Finish. A good name to use is "HTTP".
10. Repeat steps 1 thru 9 above using a port value of 443 and the name "HTTPS".

NOTE	It is also possible to turn off the firewall completely but **NOT RECOMMENDED.**

3.6.5 CONFIGURING IIS TO USE LDAP (WINDOWS SERVER 2012 AND SERVER 2012 R2)

1. Under Administrative Tools, start Internet Information Services (IIS).
2. In the left panel, select Sites -> Default Web Site.
3. In the middle panel, open Authentication under Security.
4. Set Windows Authentication to Disabled.
5. If Forms Authentication is listed, set it to Disabled.
6. If Anonymous Authentication is listed, set it to Enabled.
7. In the left panel, select Sites -> Default Web Site -> NTLM.
8. In the middle panel, open Authentication under Security.
9. Set Windows Authentication to Enabled.
10. If Forms Authentication is listed, set it to Disabled.
11. If Anonymous Authentication is listed, set it to Disabled.
12. Exit IIS Manager.

3.6.6 CONFIGURE IIS FOR SECURE CONNECTIONS (WINDOWS SERVER 2012 AND SERVER 2012 R2)

By default, IIS accepts only non-secure connections (http protocol). IIS can be configured to accept secure connections (https protocol) using Secure Sockets Layer (SSL) in addition to non-secure connections. IIS can also be configured to accept only secure connections.

In addition to configuration IIS, the web server will also need a certificate. If you do not have a certificate, one will need to be created. You can either create a self-signed certificate or obtain a certificate from a recognized Certificate Authority (CA). For information on how to create a self-signed certificate, go to http://msdn.microsoft.com/en-us/library/bfsktky3(v=vs.90).aspx. For information about how to obtain a certificate from a recognized Certificate Authority (CA), contact your administrator.

Configure Windows Server 2012 and Server 2012 R2 IIS to Accept Secure Connections as follows:

1. Under Administrative Tools, start Internet Information Services (IIS).
2. Select the Cattrax Web website in the left panel. Unless a custom directory was selected during the installation, it will be "Default Web Site".
3. Right click on the tree node and select "Edit Bindings".
4. Click the "Add..." button.
5. Select "https" in the "Type:" drop-down list.
6. Select your SSL certificate in the "SSL certificate:" drop-down list.
7. Leave the other values text boxes unchanged unless given different values by your administrator.
8. Click the "OK" button to close the "Add Site Binding" dialog box.
9. Click the "Close" button to close the "Site Bindings" dialog box.

To also disable non-secure connections, continue with these steps:

10. Ensure the website node is still selected in the left panel.
11. Double click the "SSL Settings" item.
12. Check the "Require SSL" checkbox.

For more information on enabling secure connections in Windows Server 2012 and Server 2012 R2, refer to http://www.iis.net/learn/manage/configuring-security/how-to-set-up-ssl-on-iis.

3.6.7 TEST CATTRAX WEB OPERATION

Upon completion of installation, test Cattrax Web operation in accordance with paragraph 3.9.

3.7 CATTRAX WEB INSTALLATION STEPS FOR MICROSOFT WINDOWS SERVER 2016

NOTE	**An active connection to the internet may be required for completion of the installation steps in the following paragraphs. If the PC or server device on which you are installing Cattrax Web will be used in a facility where internet access is not available, PESA recommends that you complete and test installation of the software before installing the device in the secure area.**

3.7.1 INSTALL CATTRAX WEB APPLICATION (WINDOWS SERVER 2016)

1. Login with Administrator privilege to the server on which you wish to install Cattrax Web.
2. Start the Server Manager.
3. Click Add Roles and Features.
4. On Before You Begin, click Next.
5. On Installation Type, select the correct choice for your system and click Next.
6. On Server Selection, select the correct choice for your system and click Next.
7. On Server Roles, select Web Server (IIS).
8. If a Dialog appears asking permission to install additional features, check the box "Include management tools" and then click "Add Features"; otherwise, proceed to Step 9.
9. Click Next.
10. On Features, check the box ".NET Framework 3.5 Features".
11. Expand .NET Framework 3.5 Features.
12. Check the box to enable HTTP Activation.
13. If a Dialog appears asking permission to install additional features, check the box "Include management tools" and then click "Add Features"; otherwise, proceed to Step 14.
14. Expand .NET Framework 4.6 Features, expand WCF Services, and check to enable HTTP Activation.
15. If a Dialog appears asking permission to install additional features, check the box "Include management tools" and then click "Add Features"; otherwise, proceed to Step 16
16. Click Next.
17. On Web Server Role (IIS), click Next.
18. In the left panel, select Role Services, expand Web Server, and expand Security.
19. Check Basic Authentication.
20. Check Windows Authentication.
21. Click "Next".
22. On confirmation, click Install.
23. When finished, click "Close".
24. Click Add Roles and Features.
25. On Before You Begin, click Next.
26. On Installation Type, select the correct choice for your system and click Next.
27. On Server Selection, select the correct choice for your system and click Next.
28. On Server Roles, expand Web Server (IIS), expand Web Server, expand Application Development, and check the box to enable ASP.NET 3.5.
29. Click Next.
30. On Features, click Next.

31. On confirmation, click Install.
32. When finished, click "Close".
33. Exit Server Manager.
34. Under Administrative Tools, start Internet Information Services (IIS).
35. In the left panel, expand the local computer name.
36. Click the Application Pools entry.
37. In the middle panel, Application Pools, select the DefaultAppPool entry.
38. In the right panel under Edit Application Pool, click Advanced Settings.
39. In the dialog, ensure that General -> Enable 32-Bit Applications is set to True.
40. Scroll down to Recycling -> Specific Times.
41. Click the … item to the right of TimeSpan[] Array.
42. If a textbox is not displayed in the left column, click Add.
43. Enter a specific time of day, such as 01:00:00 for 1 AM in the field next to Value. Select a time of day which is low demand.
44. Click OK to accept the time value entered.
45. Click OK to close the Advanced Field Settings dialog.
46. In the left panel, select Sites -> Default Web Site.
47. In the right panel under Actions, click Basic Settings.
48. Ensure that "%SystemDrive%\intepub\wwwroot "or "C:\intepub\wwwroot" is in the text box Physical path.
49. Ensure that the Application Pool is set to DefaultAppPool.
50. Click OK to close the Edit Site dialog.
51. Exit IIS Manager.
52. Insert the Cattrax Web installation disk.
53. Run *Cattrax Web Prerequisites Setup.exe*, click *Next* when prompted. On the *Choose Components* page, leave all boxes checked unless instructed otherwise by PESA Customer Service. Select *Install* to continue with installation.

    While running the Prerequisites installation disk, if the installer application requests a restart of the computer, follow these guidelines:

    - Respond "Yes" to allow the computer to reboot if the installer asks permission.
    - Run the *Cattrax Web Prerequisites Setup.exe* file again after any reboots. This ensures all prerequisites are installed.

54. Click *"Finish"* to complete installation of Prerequisites.
55. Run *Cattrax Web x.x.x Setup.exe*, click *Next* at the initial prompt. You will be asked to read and agree to the terms of the Cattrax Web software license. Click *"I Agree"* to continue with installation.

56. On the *Choose Components* page, leave all three boxes checked unless instructed otherwise by PESA Customer Service. Click *"Next"* to continue to the *"Choose Installation Location"* prompt.
57. Use of the default install location is recommended; however, you may change the default location in the "Choose Install Location" page of the wizard. Be aware, that choosing a location that is outside the wwwroot directory might interfere with access to the Cattrax Web website. Click *"Install"* to begin the installation process.
58. If an error is reported on "Accumulated Updates" or "database update", repeat Steps 55 and 56, above.
59. If a prompt is displayed requesting a restart of Cattrax Web if it is running, click OK.
60. A progress bar allows you verify installation. Upon completion, you will be prompted to click *"Finish"* to complete the installation process.
61. Under Administrative Tools, open Internet Information Services (IIS).
62. In the left panel, expand the local computer name, expand *Sites*.
63. Double click *Sites -> Default Web Site.*
64. Double click the *CSS* directory.
65. Right click the *Images* directory and select *"Edit Permissions…"*.
66. Select the *Security* tab.
67. Click *Edit.*
68. Select *ASP.NET Machine Account*. If that entry is not listed, select *"IIS_USERS"*.
69. Click the *Write* check box in the *Allow* column.
70. Click OK.
71. Click OK to close the *Edit* dialog.
72. Click OK to close the *Properties* dialog.

On 64-bit systems, you will need to configure IIS to run 32-bit applications, as follows:

1. Under Administrative Tools, start Internet Information Services (IIS).
2. Expand the first node on the *Connections* panel and click *Application Pools*.
3. Right-click *DefaultAppPool*, select Advanced Settings, and change *Enable 32-Bit Applications* to *True*, if that option is not already selected.
4. Click OK.

3.7.2 CUSTOM DIRECTORY (WINDOWS SERVER 2016)

The default installation directory is: c:\InetPub\wwwroot. **Use of this directory is recommended**.

A custom installation directory may also be selected. For example: c:\MySites\CattraxWeb. This should be used if another website is already installed in the root directory.

After changing the default directory, configure a virtual directory as follows:

1. Under Administrative Tools, start Internet Information Services (IIS).
2. In the left panel, select Sites -> Default Web Site.

3. In the right panel under Actions, click Basic Settings.
4. Enter the path you want to use in the text box Physical path.
5. Click OK to close the Edit Site dialog.
6. Exit IIS Manager.

3.7.3 SETTING THE IIS RECYCLING TIME AND IDLE TIMEOUT (WINDOWS SERVER 2016)

In order to set the recycling time through Windows Server 2016 use the following procedure:

1. Under Administrative Tools, start Internet Information Services (IIS).
2. On the left side of the window under "Connections", expand the local computer name.
3. Click the *Application Pools* entry.
4. In the middle panel, Application Pools, select the *DefaultAppPool* entry.
5. In the right panel, select the *Set Application Pool Defaults* entry.
6. In the dialog under Process Model, edit the Idle Time-out. Enter a value such as 480 minutes.

   NOTE: The "minutes" value entered will set the amount of time during which the CattraxWeb application will not be unloaded by IIS if no user command is received, such as changing which page is displayed, entering data, or making a switch. Using the example of 480 minutes will set the Idle Time-out at 8 hours.
7. Scroll down to the *Recycling* entry.
8. Under *Regular Time Interval*, set the value to zero (0).
9. Click the "…" item in the right side of the *Specific Times* entry.
10. Click *Add* in the dialog.
11. Enter a specific time of day, such as 01:00:00 for 1 AM. Select a time of day which is low demand.
12. Click *OK* to accept the time value entered.
13 Click *OK* to close the dialog.
14. Reboot the server to activate settings.

3.7.4 CONFIGURE WINDOWS FIREWALL (WINDOWS SERVER 2016)

Use this procedure if you are using the Windows Firewall in Windows Server 2016 in the Cattrax Web host server:

1. Under *Administrative Tools*, run *Windows Firewall with Advanced Security.*
2. In the left panel, click *Inbound Rules.*
3. In the right panel, click *New Rule.*
4. In *Rule Type* window, select *Port* and click Next.
5. In the *Program* window, select *All Programs* and click Next.
6. In *Protocol and Ports*, select *TCP and Specified local ports*, and set the port value to 80 and click Next.

7. In *Action*, select *Allow the Connection* and click Next.
8. In *Profile*, select all items (or as appropriate based on who would have access to Cattrax Web) and click Next.
9. In *Name*, give this rule a name and optionally a description and click on Finish. A good name to use is "HTTP".
10. Repeat steps 1 thru 9 above using a port value of 443 and the name "HTTPS".

NOTE	It is also possible to turn off the firewall completely but **NOT RECOMMENDED.**

3.7.5 CONFIGURING IIS TO USE LDAP (WINDOWS SERVER 2016)

1. Under Administrative Tools, start Internet Information Services (IIS).
2. In the left panel, select Sites -> Default Web Site.
3. In the middle panel, open Authentication under Security.
4. Set Windows Authentication to Disabled.
5. If Forms Authentication is listed, set it to Disabled.
6. If Anonymous Authentication is listed, set it to Enabled.
7. In the left panel, select Sites -> Default Web Site -> NTLM.
8. In the middle panel, open Authentication under Security.
9. Set Windows Authentication to Enabled.
10. If Forms Authentication is listed, set it to Disabled.
11. If Anonymous Authentication is listed, set it to Disabled.
12. Exit IIS Manager.

3.7.6 CONFIGURE IIS FOR SECURE CONNECTIONS (WINDOWS SERVER 2016)

By default, IIS accepts only non-secure connections (http protocol). IIS can be configured to accept secure connections (https protocol) using Secure Sockets Layer (SSL) in addition to non-secure connections. IIS can also be configured to accept only secure connections.

In addition to configuration IIS, the web server will also need a certificate. If you do not have a certificate, one will need to be created. You can either create a self-signed certificate or obtain a certificate from a recognized Certificate Authority (CA). For information on how to create a self-signed certificate, go to http://msdn.microsoft.com/en-us/library/bfsktky3(v=vs.90).aspx. For information about how to obtain a certificate from a recognized Certificate Authority (CA), contact your administrator.

Configure Windows Server 2016 IIS to Accept Secure Connections as follows:

1. Under Administrative Tools, start Internet Information Services (IIS).
2. Select the Cattrax Web website in the left panel. Unless a custom directory was selected during the installation, it will be "Default Web Site".

3. Right click on the tree node and select "Edit Bindings".
4. Click the "Add..." button.
5. Select "https" in the "Type:" drop-down list.
6. Select your SSL certificate in the "SSL certificate:" drop-down list.
7. Leave the other values text boxes unchanged unless given different values by your administrator.
8. Click the "OK" button to close the "Add Site Binding" dialog box.
9. Click the "Close" button to close the "Site Bindings" dialog box.

To also disable non-secure connections, continue with these steps:

10. Ensure the website node is still selected in the left panel.
11. Double click the "SSL Settings" item.
12. Check the "Require SSL" checkbox.

For more information on enabling secure connections in Windows Server 2016, refer to http://www.iis.net/learn/manage/configuring-security/how-to-set-up-ssl-on-iis.

3.7.7 TEST CATTRAX WEB OPERATION

Upon completion of installation, test Cattrax Web operation in accordance with paragraph 3.9.

3.8 HOW TO MOVE A CATTRAX WEB DATABASE FROM A COMPUTER WITH SQL SERVER 2008R2 (WINDOWS XP/7/10) TO A COMPUTER WITH SQL SERVER 2014 (WINDOWS SERVER 2012 AND LATER).

On the computer you are moving the database from:

1. Backup the database on the CattraxWeb as described in section 5.15.
2. Copy the database backup file from the database backup directory (probably *C:\ProgramData\PESA\Cattrax Web\DatabaseBackup*).

On the computer you are moving the database to:

1. Put the copied database backup file (database1.2.3.bak in this example) in the database backup directory, probably *C:\ProgramData\PESA\Cattrax Web\DatabaseBackup.*
2. Edit the file *C:\inetpub\wwwroot\Help\CopyToSQL2014.template*. Change the database path and filename in line 4 to the actual path and filename for your database file. If the path to MSSQL12 is different on your system, change that also. Save the file as *CopyToSQL2014.sql* in the database backup directory, probably *C:\ProgramData\PESA\Cattrax Web\DatabaseBackup.*
3. Open a command prompt window.
4. Go to the database backup directory, probably *'C:\ProgramData\PESA\Cattrax Web\DatabaseBackup.*
5. Execute the command below:

   sqlcmd -S .\SQLPESA -i " CopyToSQL2014.sql"

6. Execute the command below. If the path to MSSQL12 is different, change that. If there is an error, try the command again:

   C:\Program Files (x86)\Microsoft SQLServer\MSSQL12.SQLPESA\MSSQL\DATA\accumulatedUpdates.sql

7. Execute the command below:

   iisreset /restart

3.9 TESTING CATTRAX WEB INSTALLATION

After installation of Cattrax Web is complete, open an internet browser such as Mozilla Firefox, or Google Chrome and connect to the Cattrax Web URL as follows:

- To connect from a browser running on the Cattrax Web server computer, if you allowed Cattrax Web to install in the default root directory – use URL http://<Server IP Address> to connect to Cattrax Web from the internet browser. For example: http://192.168.20.123, or simply http://localhost.
- To connect from a browser running on the Cattrax Web server computer, if you installed Cattrax Web in a custom root directory – use URL http://<Server IP Address>/CattraxWeb to connect to Cattrax Web from the internet browser. For example: http://192.168.20.123/CattraxWeb, or simply http://localhost/CattraxWeb. This example assumes a custom directory named "CattraxWeb" was used for application installation. If you used any other custom name – enter the actual directory name in the URL in place of CattraxWeb.
- To connect from a browser running on a computer different from the Cattrax Web server computer, if you allowed Cattrax Web to install in the default root directory – enter the URL as the IP address of the computer hosting the Cattrax Web application, as shown here: http://<Server IP Address>.
- To connect from a browser running on a computer different from the Cattrax Web server computer, if you installed Cattrax Web in a custom root directory – enter the URL as shown here: http://<Server IP Address>/CattraxWeb. This example assumes a custom directory named "CattraxWeb" was used for application installation. If you used any other custom name – enter the actual directory name in the URL in place of CattraxWeb.

The Cattrax Web login page should be shown.

If Cattrax Web does not respond, you need to ensure that the network Firewall in the computer on which Cattrax Web is installed, allows the http:// requests to pass through. The configuration of the firewall depends on the firewall hardware or software in use. Refer to paragraph 3.4.4, as applicable to your server operating system.

3.10 CONFIGURING THE FIREFOX BROWSER TO USE LDAP

When using LDAP login options, the Mozilla Firefox browser will prompt for a login box. To prevent this, make the following settings:

1. Go to **about:config.**
2. Set **network.automatic-ntlm-auth.allow-non-fqdn** to **true.**

3.11 CATTRAX WEB APPLICATION – UNINSTALL

The *Cattrax Web x.x.x Setup.exe* program will prompt you to uninstall the previous version if it detects a version of Cattrax Web already installed. It is not mandatory to uninstall the previous version; however, it is recommended that you do.

	Uninstall only removes some of the Cattrax Web application files from the c:\inetpub\bin directory. It does not uninstall the database server, the Cattrax Web database, any backed up database files and log files, or the SMTP mail settings.

Chapter 4 Initial Login and Setup

4.1 Initial Login and License Activation

With the Cattrax Web server application installed and running on the host computer, initial steps to prepare for operation are to login to Cattrax Web using the pre-configured, default ***Admin*** user account, activate the software license, change password and security question of the default user account, and (recommended, but not required) create a new administrator level user account to use for common and routine administrative functions.

The procedures in this chapter should only be required at initial setup of the Cattrax Web application. Refer to Chapter 5 for normal operating procedures.

Start your web browser application and enter the URL of the Cattrax Web server to access the login page, as shown by Figure 4-1.

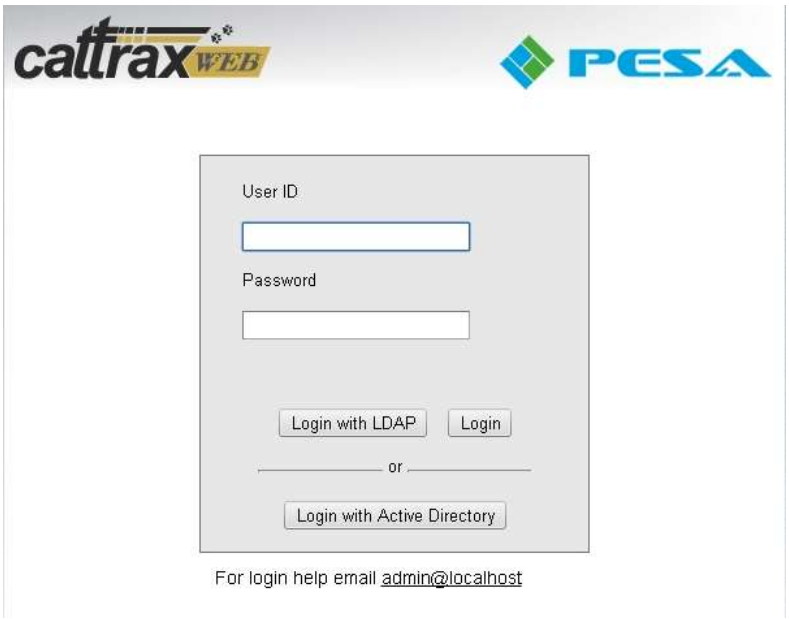


Figure 4-1 Cattrax Web Login Page

For the initial login you must use the factory default login credentials: User ID is ***admin*** and default Password is ***admin*101***. Enter these credentials and click the *Login* button to login to Cattrax Web.

You must activate the software license before any functions of Cattrax Web are accessible or operational. If this is the first time the application has been accessed following installation, the program opens to the Software License activation page, Figure 4-2. Follow the procedures in paragraph 4-2 to install the license and activate Cattrax Web.

4.2 Activate Software License Key

Activation of the Software License Key opens access to operational features of Cattrax Web, and also configures the number of simultaneous users that may be logged in to the application. Until the software license is activated, Cattrax Web opens by default to the Software License activation page, Figure 4-2, at login.

An activation key provided by PESA is required for initial setup, and may be a system-specific key or a test key. A test key is for evaluation of the Cattrax Web application and expires after a specified number of days. Both keys are activated by the following procedure:

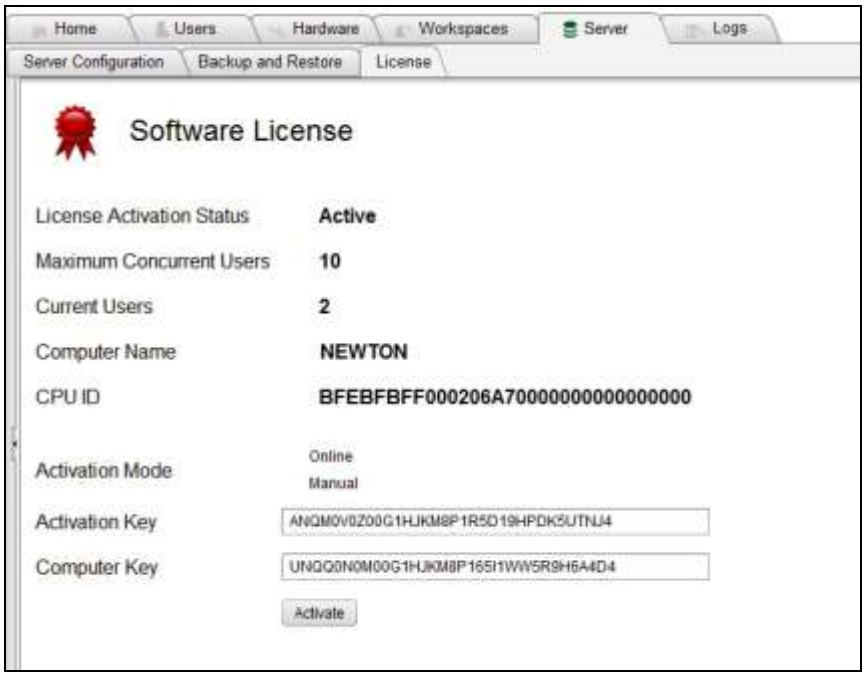


Figure 4-2 License Activation Page

NOTE	1. The *Maximum Concurrent Users* displayed in a license defines the number of simultaneous user sessions allowed. It is possible to add any number of users to the Users List page. 2. If the same user logs in from two different browsers Cattrax Web considers this to be two simultaneous sessions. 3. When a user logs out, current simultaneous user count is decremented immediately. If the user doesn't log out, the current user count is decremented after user inactivity timeout. Inactivity timeout may be set from the Server Configuration page, see paragraph 5.13.

4.2.1 ONLINE ACTIVATION

- If the server (host computer) on which Cattrax Web is installed has access to the internet, select the *Online* Activation Mode.
- Enter the Activation Key (provided by PESA) in the Activation Key window and click the *Activate* button.
- Cattrax Web communicates with PESA's License Server over the internet connection and registers the CPU ID and Name of your host computer against the activation key and immediately obtains a Computer Key from PESA.

- If activation is successful, the computer key character string is displayed along with the maximum number of simultaneous sessions allowed by this key.
- Upon completion of activation, the message *Valid Key(s)* is displayed in the lower left area of the Key Activation window. Once this message appears, Cattrax Web is fully functional.
- When you have completed the licensing process, you will be logged into Cattrax Web through the default ***Admin*** user account. Click the **Home** tab at the top of the license page to access the **Setup** home page.
- Although this step is not a requirement for operation of the application, for security reasons PESA recommends changing the password of the ***Admin*** user account before you perform any other function with Cattrax Web. Refer to paragraph 4.3.
- PESA also recommends that while you are logged in through the ***Admin*** user account, you create a new Administrator level User ID and Password for day-to-day administrative use. Refer to paragraph 4.4.

NOTE	If online activation of a *test key* fails you will still be able to the use the number of sessions allowed by the key.

4.2.2 MANUAL (OFFLINE) ACTIVATION

- If access to the internet is not available, select the *Manual* Activation Mode.
- Make a notation of the Computer Name and CPU ID character string as displayed on the License Activation page.
- Send the name and ID number to PESA. You may use Email, or contact PESA Customer Service by phone to obtain your activation information.
- PESA will issue to you a Computer Key character string.
- Once you have received the Computer Key, enter both the Activation Key that you received with Cattrax Web AND the Computer Key issued to you by PESA in the appropriate data entry fields on the License Activation page, and click the *Activate* button.
- If activation is successful, the computer key character string is displayed along with the maximum number of simultaneous sessions allowed by this key.
- Upon completion of activation, the message *Valid Key(s)* is displayed in the lower left area of the Key Activation window. Once this message appears, Cattrax Web is fully functional.
- When you have completed the licensing process, you will be logged into Cattrax Web through the default ***Admin*** user account. Click the **Home** tab at the top of the license page to access the **Setup** home page.
- Although this step is not a requirement for operation of the application, for security reasons PESA recommends changing the password of the ***Admin*** user account before you perform any other function with Cattrax Web. Refer to paragraph 4.3.
- PESA also recommends that while you are logged in through the ***Admin*** user account, you create a new Administrator level User ID and Password for day-to-day administrative use. Refer to paragraph 4.4.

4.3 CHANGE THE PASSWORD AND SECURITY QUESTION OF THE ADMIN USER ACCOUNT

PESA recommends for added security that during initial setup you change the password of the ***Admin*** user account from the default ***admin*101*** to a password that is unique for your installation. It is also recommended that you change the security question and answer for the account as well.

NOTE	User ID ***Admin*** cannot be removed from the system through the User List page. The privilege level of *Admin* is permanently set to administrator and cannot be changed.

All administrative and setup functions of Cattrax Web are done through pages available from the Setup home page. An example page is shown by Figure 4-3.

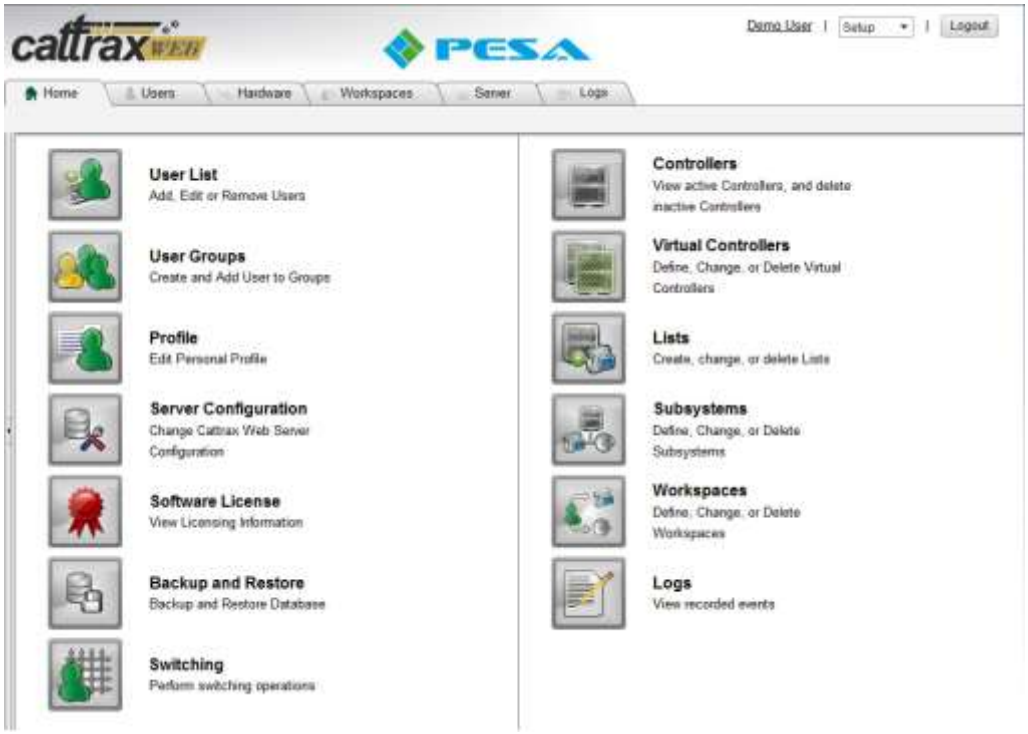


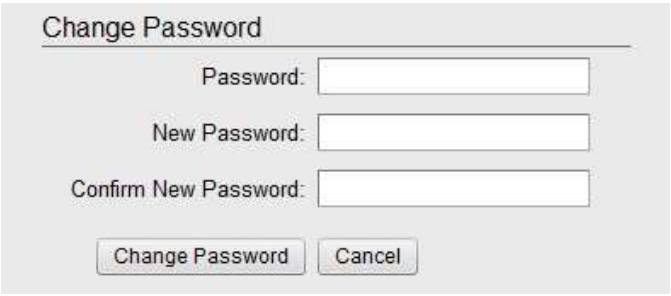
Figure 4-3 Cattrax Web Setup Home Page

Change the password of the Admin user account as follows:

- Click on the **Profile** icon located in the left column of the home page. You can also access the User Profile page at any time by clicking the User ID display in the top right corner of the page. In Figure 4-3, the User ID is shown as *Demo User*. An example User Profile page is shown by Figure 4-4.

Figure 4-4 User Profile Page

- Click the *Change Password* link to open the Change Password dialog box as shown here. Enter the default password (***admin*101***) and then enter the new password you wish to create for the Admin user account. Confirm the new password and click the *Change Password* button.



- All passwords must be at least 7 characters long with at least one non-alphanumeric character.
- Click the *Change Security Question* link to open the Change Security Question dialog box as shown here. Enter the new password you just created for the Admin account. Enter the new security question you wish to create and enter the answer to the question in the appropriate fields. Click *Save* to complete the change process.
- Store the newly created password and security answer for User ID *Admin* in a safe place.

CAUTION	**Make a notation of the *Admin* user password and security answer, and store them in a safe location. If the password or security answer is lost, the only way to reset it would be by deleting the Admin account from the database and restarting the web application. Do not attempt to alter the database without assistance from PESA service personnel, Contact PESA Customer Service if you ever need to delete the Admin account from the database.**

4.4 CREATE A NEW USER ACCOUNT WITH ADMINISTRATOR PRIVILEGE

Although not a requirement for system operation, PESA recommends that while logged in through the factory default ***Admin*** user account, you create a new administrative user account for use as a top level system administrator account for Cattrax Web operations. Once the new account is created, log in to Cattrax Web with the newly created User ID and Password and use this account for initial system setup, routine maintenance and administrative operations, rather than using the default ***Admin*** account. Create the new user account as follows:

- Return to the Setup home page, Figure 4-3 and click the **User List** icon (left column) to open the User List page as shown by Figure 4-5.

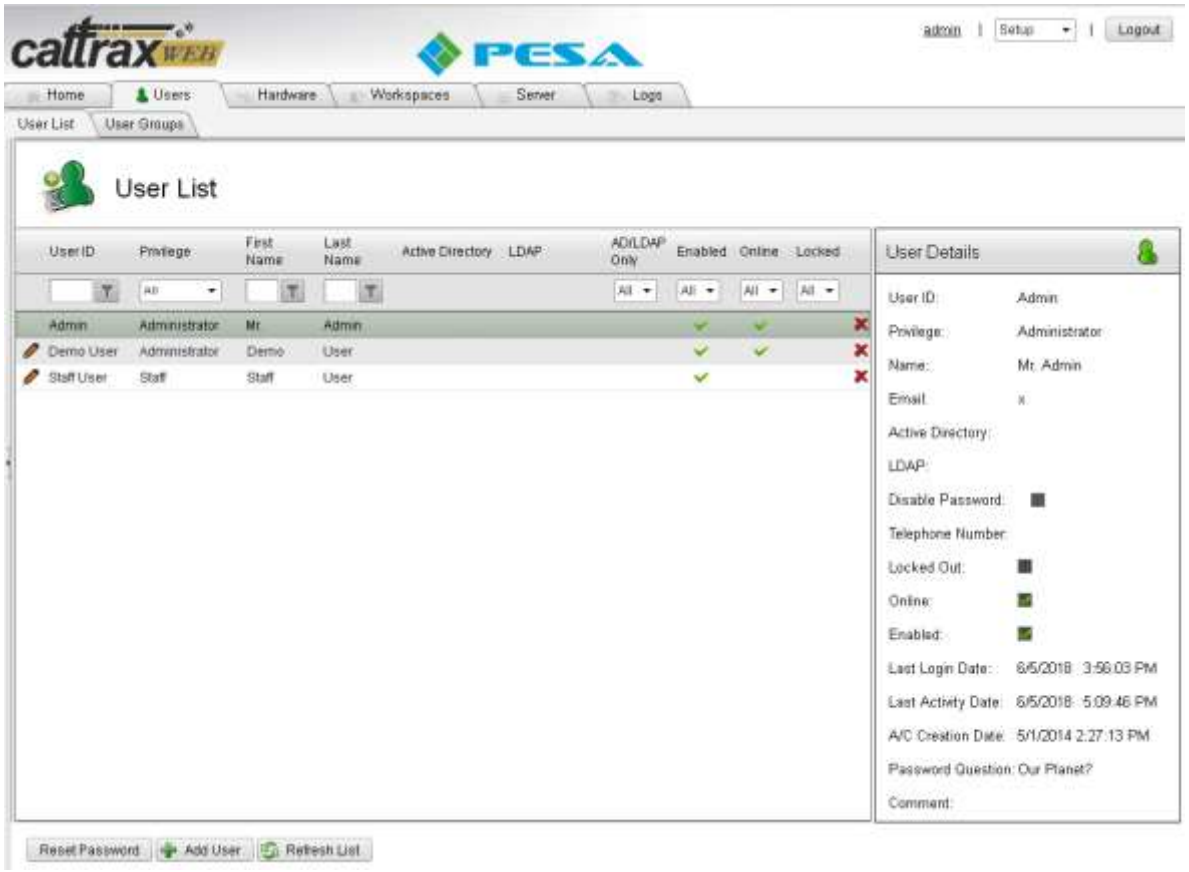
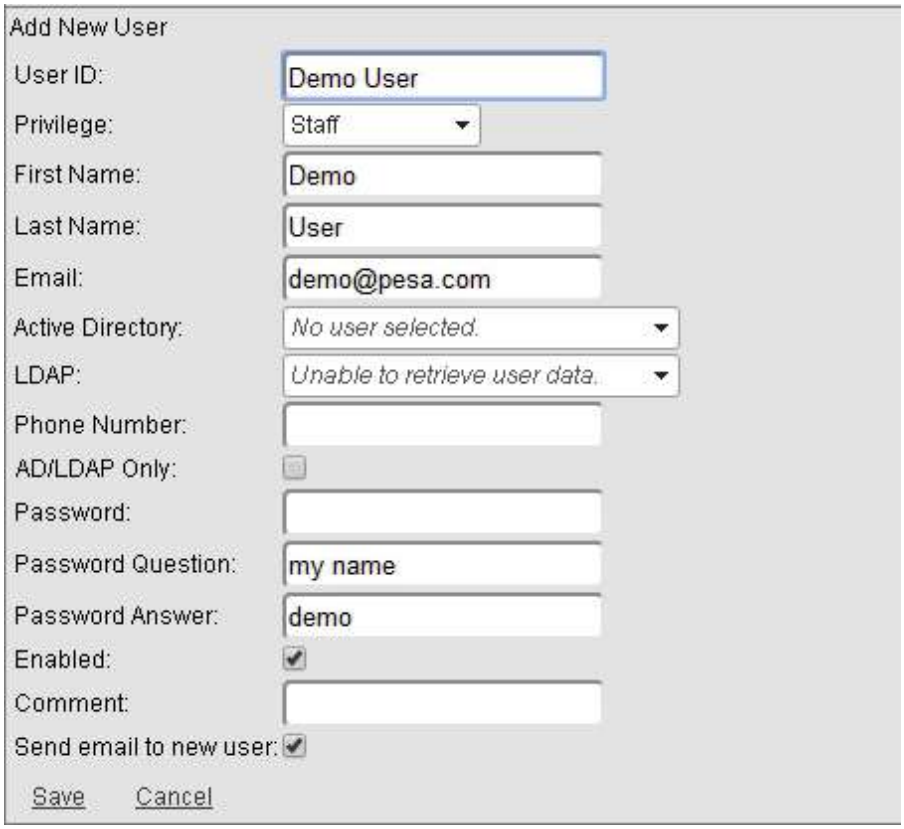


Figure 4-5 User List Page

- Click the *Add User* button to access the **Add New User** dialog box as shown below.
- Enter the User ID as you want it to appear in the User List, a first and last name for the new administrator account, and an Email address. For this example, we have created the User ID **Demo User**.



- Select the **Admin** access privilege level for this user from the *Privilege* drop-down list.

NOTE	Privilege level for all new users defaults to *Staff*. Since the User ID we are creating is intended as an administrator level login, change the privilege level to *Admin* from the drop-down list.

- As an optionally available feature, Cattrax Web supports user login with externally authenticated domain login credentials through either Active Directory or an LDAP server, if these network services are available on your facility's IT infrastructure. In order to use either of these login methods, you must first configure Cattrax Web to interface with these services through settings that you will enter on the Server Configuration page of the application during system set-up.

  Leave both the *Active Directory* and *LDAP* fields blank for now. If you would like to allow login to the new administrator account through either (or both) of these methods, you may edit the user page for this account once set-up of alternate login methods is complete and the services are operational. Refer to paragraph 2.2 for more information on using the alternative login methods.

- Enter a phone number for the new administrator account, if desired (optional).
- Be sure that the *AD/LDAP Only* box is **not** checked for now. If upon completion of system configuration, you would like to restrict login to the new administrator account to either (or both) of these methods, you may edit the user page for this account once set-up of alternate login methods is complete and the services are operational. Refer to paragraph 2.2 for more information on using the alternative login methods.

	When checked, the *AD/LDAP Only* checkbox restricts the user to only log in to Cattrax Web through Active Directory or LDAP network server login methods. Placing a check in this box disables the Login Page option of entering application-specific user ID and password credentials assigned to the user at the time of account creation or through subsequent user account changes to access Cattrax Web. Refer to paragraph 2.2 for more information on alternate login methods.

- Provide a password for the new administrative account and a password challenge question. You may use any question and answer you wish for password retrieval.
- Click the *Enabled* box to enable the user account you are creating and allow the user to login.
- *Comment* is a free text area where you may make any notes you wish. An entry in this area is not required to create a user account.
- If you would like to have Cattrax Web send a notification email to the new user, click the *Send email to new user* box.
- Click *Save* to create and add the new account to the user list.
- Logout from the ***Admin*** user account, using the *Logout* button at the top right corner of the screen, and login to Cattrax Web again as the new administrator level user you just created.
- When you have completed all initial licensing and setup procedures, continue to Chapter 5 for normal operating procedures.

Chapter 5 Operation

5.1 INTRODUCTION

In order to control access to various setup and configuration operations of the application, Cattrax Web functions in two essentially distinct operational areas, **Setup** and **Switching:**

- **Setup** functions allow users with administrative privilege to configure all aspects of application operation including users, router control and access, server functions and the creation of system operation and history logs.
- **Switching** functions are available to authorized users of all privilege levels and provide status display and control for the router, or partition of the router, granted to the individual user accessing the server.

  All authorized users access router control through the Switching operational area of Cattrax Web. The Switching page identifies one or more ***workspace*** instances to which the specific logged-in user has been granted access. Workspace instances are created by system administrators or supervisors to very specifically assign and control router access to individual users or user groups.

Individual users may be assigned to one of three privilege levels that determine the functions of Cattrax Web they can access and control:

- **Staff** – Staff level users are granted access to only the Switching user interface pages and functions. When a Staff level user logs in to Cattrax Web the application opens immediately to the Switching page.
- **Supervisor** – Supervisor level users are granted access to both the Switching and Setup functional areas of Cattrax Web, with the exception of the server configuration pages. Following hierarchy, a Supervisor level user cannot:
  - Create a new Administrator level user account,
  - Grant Administrator level access to a new or existing user account, or
  - Edit the account or change access privilege of any user with Administrator privilege.
- **Administrator** – Administrator level users are granted access to all pages and functions of Cattrax Web.

NOTE	Throughout this text, the term *"administrative user"* is used to differentiate both Supervisor and Administrator level users from Staff level users. When used in a procedural step, an administrative user is any user with system access privileges needed to perform the administrative control or setup functions required for the operation being discussed.

Each operational area is discussed in the following paragraphs. Regardless of privilege level, all users open the application through the Login page.

5.2 LOGIN TO CATTRAX WEB

Start your web browser application and enter the URL of the Cattrax Web server to access the login page, as shown by Figure 5-1.

Figure 5-1 Cattrax Web Login Page

Enter your User ID and Password, and click the Login button.

5.3 LANDING PAGE

The privilege level of the user logging in to Cattrax Web determines the initial landing page the user will see.

If you log in with a user ID assigned a privilege level of Supervisor or Administrator, Cattrax Web will automatically open to the **Setup** home page. Refer to paragraph 5.4

Staff level users do not have access to the Setup operational pages, and for these users Cattrax Web will automatically open to the **Switching** home page. Refer to paragraph 5.18.

Regardless of which landing page is open, there are three user controls at the top-right of the page as shown by the example illustration at right.

Username – The User ID of the currently logged-in user is shown underlined. Click the username display to quickly access the individual profile page for that user. You may make any changes you wish to the user profile information from the profile page.

Operational Area Select – The pull-down list allows you to easily move between the **Setup** home page and the **Switching** home page. Open the pull-down list and select the page you wish to access. The **Setup** page selection is not available to Staff level users.

Logout – Click the logout button to log the current user out of Cattrax Web. The application will open to the Login page and allow another user to log in to the application, if desired. Anytime a user logs out of the application, the simultaneous sessions count will be decremented by one.

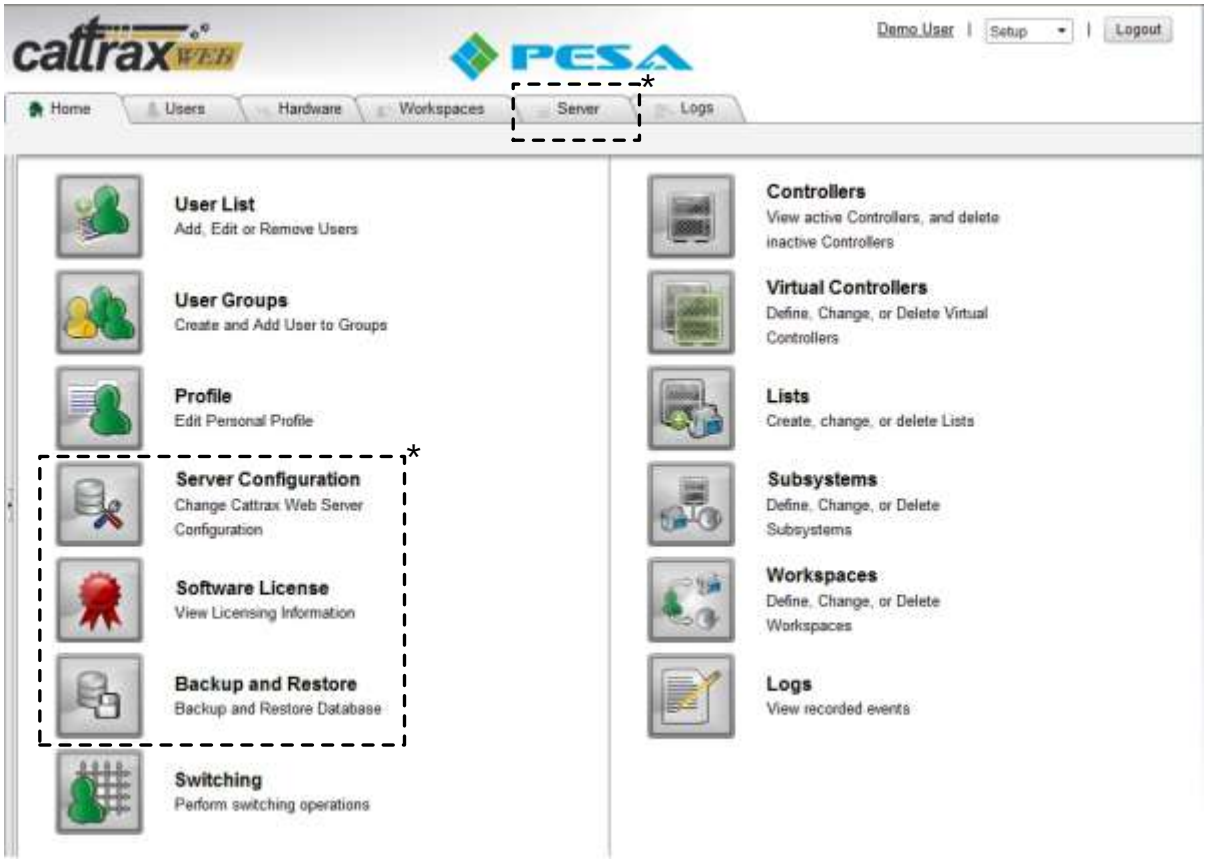
5.4 SETUP HOME PAGE

System configuration and setup functions available to the user are listed in columns on the Setup home page and also identified by icons, as shown by Figure 5-2. Click any function header or icon on the page to open its associated control or configuration page.

A user assigned the privilege level of Administrator can access any functional area of Cattrax Web and perform any system operation or command.

Users assigned the privilege level of Supervisor can perform most of the same control functions as an Administrator. A supervisor level user may not access or change the network configuration of Cattrax Web, make any changes to the server operating parameters, assign a user administrator privileges or modify the status of an administrator level user.

Control functions available through the Setup home page are discussed in the following paragraphs.



* Icons and menu tab enclosed by dotted lines are not displayed on the Setup home page of a Supervisor level user

Figure 5-2 Setup Home Page

Tabs across the top of the main display area, as shown below, allow quick access to user interface pages for the various control functions.

There is also a row of sub-tabs for Users, Hardware, and Server tabs that give access to various pages under each category.

5.5 CONFIGURE DEVICE NETWORK (ADMINISTRATOR LEVEL USER)

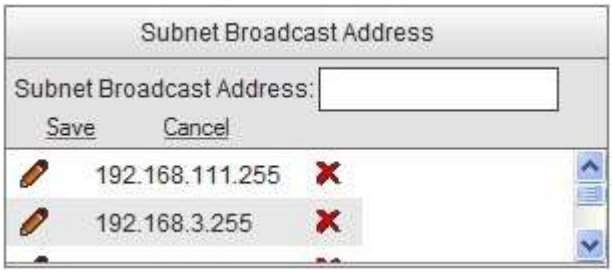
Before any router control functions or communication with the system controller can be implemented, Cattrax Web requires configuration of the device network in order to allow the application to "discover" the presence of PESA devices on the network. Configure device network information as follows:

- From the Setup home page, Figure 5-2, click the *Server Configuration* icon (left column) to open the Server Configuration page as shown by Figure 5-3.

Figure 5-3 Server Configuration Page

Cattrax Web should automatically discover the active network interface device of the host server (host PC) and automatically add the Subnet Broadcast Address to the list. This address is valid for discovering devices on the same subnet as the Cattrax Web server. If there are also PESA devices on a different subnet, the subnet broadcast address for that subnet must be manually added to the list as follows:

- Click the *Add Subnet* button to add a new subnet. A pop-up dialog box prompts you for the broadcast address of the subnet you wish to add, as shown at right.
- Enter the new address and click the *Save* button to add it to the list.
- Click *Cancel* to exit the box without any changes to the list.



Recommendation: Use the subnet broadcast address from the Network Preference settings dialog of Cattrax.

5.6 OVERVIEW OF ADMINISTRATIVE FUNCTIONS

Cattrax Web administrative controls and functions may be loosely divided into four categories:

1. **User Configuration -** Add, edit and delete user accounts, assign user access privilege and create user groups.
2. **Hardware Configuration -** Add, edit and delete virtual controllers, system resource include lists and subsystems.
3. **Workspace Configuration -** Add, edit and delete workspaces; and assign users to their authorized workspace(s).
3. **Server Administration -** Includes various configuration and maintenance functions of the Cattrax Web server, such as device network configuration, Email configuration, system log management, etc.

Each function is performed through interactive user interface pages. Many pages incorporate a table format to display and sort data content of the page. An example of the table display format is shown by Figure 5-4. With many of the tables, each display row will feature a pencil icon on the left edge and a *red "X"* icon on the right edge. When the data entry row is selected (highlighted), clicking the pencil icon brings up a dialog box that allows you to edit certain fields of the entry, and clicking the *red "X"* icon allows you to delete the entry.

Many of the table columns feature data search and sort capability. At the top of table columns that offer such capability, a data entry box allows you to enter the character or character string you wish to locate in the column. Clicking the filter icon next to the data entry box opens a drop-down menu listing of criteria you may use to refine your search.

You may sort the content of columns that offer sorting capability by clicking the column name header. The column header *User ID* for example, sorts the table in alphabetical order based on the entries in the User ID column. Clicking the header again, reverses the order of sorting.

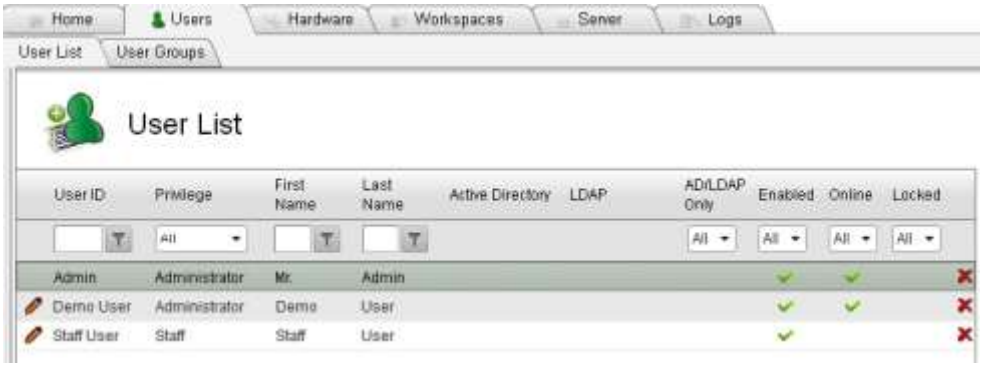


Figure 5-4 Table Display Format

5.7 USER CONFIGURATION

There are three main objectives of user configuration:

1. Manage user access to the Cattrax Web application.
2. Manage access level privileges assigned to each user.
3. Assign users to specific user groups (optional).

5.7.1 USER LIST PAGE

The User List page, Figure 5-5, provides information about users with a Cattrax Web account. Access the page by clicking the *User List* icon on the Setup home page, or by selecting the *Users* tab on the menu bar and clicking the sub-tab *User List*. From the User List page, administrative users may, within the authority of their access privileges, add new users, edit or delete existing user accounts, change system access privilege for a user, enable or disable user access to the application, and reset user passwords and lock-outs.

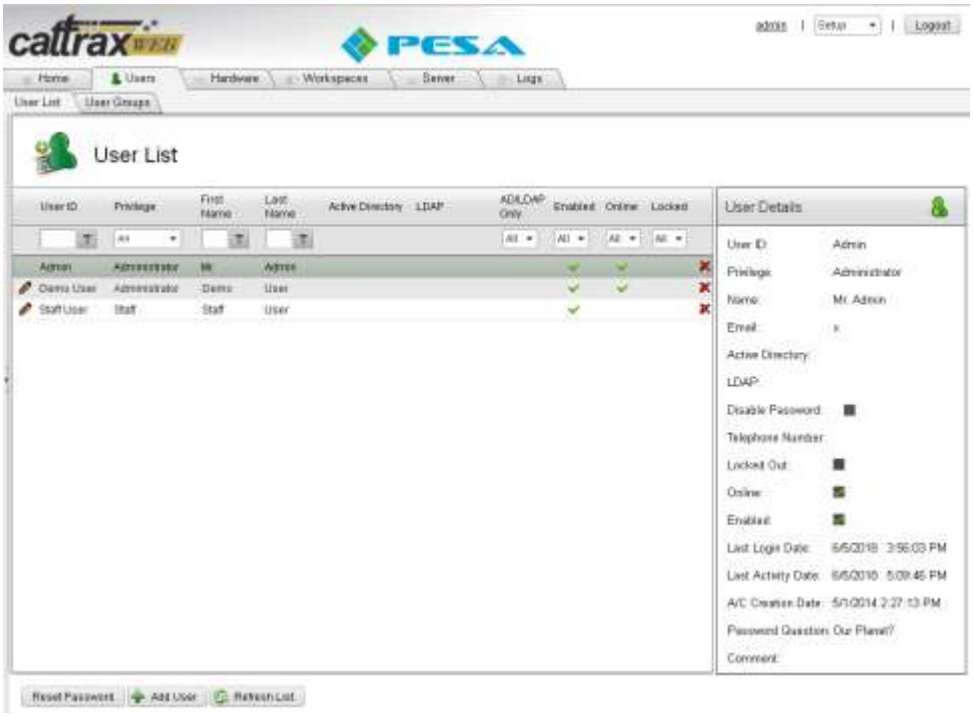


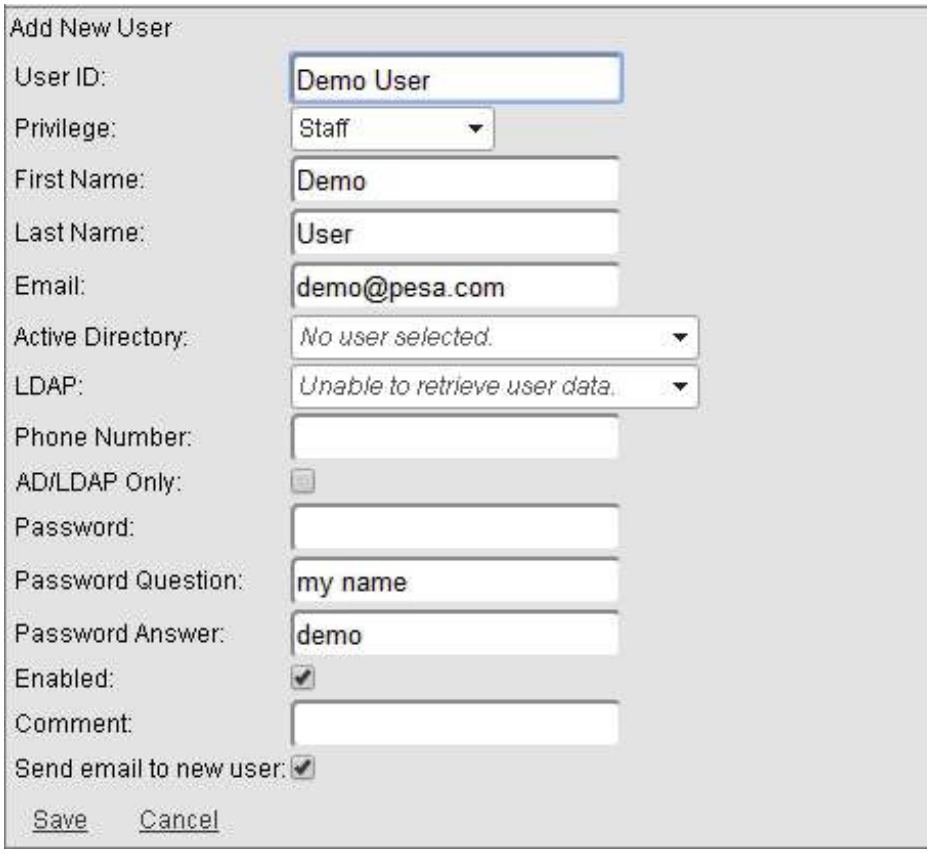
Figure 5-5 User List Page

Add or Create User Accounts

User accounts may be created by either of two possible methods:

- If the function is enabled through server configuration, a new user may request an account through the *New User Registration* link on the login page
- An administrative user may create a new user account through the User List page. A Supervisor level user can not assign a new user the level of Administrator.

Administrative users can add user accounts through the User List page by clicking the *Add User* button beneath the user table to open an empty **Add New User** dialog box, as shown below. Enter the data requested for each field, as introduced in the following steps. Check the *Enabled* box and click *Save* to create and activate the new account.

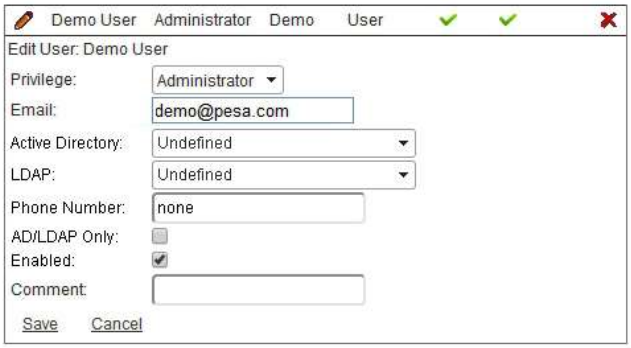


- Enter the User ID as you want it to appear in the User List, the first and last name of the user, and the user Email address. For this example, we are using the User ID **Demo User**.
- Select the system access privilege level you wish to allow this user from the *Privilege* drop-down list.

- If Cattrax Web is configured to support user login through either Active Directory or an LDAP server, you may associate the Cattrax Web user's account to a user ID on the facility network for login access by opening the drop-down list in the appropriate field (*Active Directory* or *LDAP*) to display a network user ID listing. Highlight the desired ID from the list and click. Refer to paragraph 2.2 for more information on alternate login methods.
- Enter a phone number for the user, if desired (optional).
- When checked, the *AD/LDAP Only* checkbox restricts the user to only log in to Cattrax Web through Active Directory or LDAP network server login methods. Placing a check in this box disables the Login Page option of entering application-specific user ID and password credentials assigned to the user at the time of account creation or through subsequent user account changes to access Cattrax Web. Refer to paragraph 2.2 for more information on alternate login methods.
- Provide a password for the user and a password challenge question. You may use any question and answer you wish for password retrieval.
- Click the *Enabled* box to enable the user account you are creating and allow the user to login.
- *Comment* is a free text area where you may make any notes you wish. An entry in this area is not required to create a user account.
- If the *Send email to new user* check box is checked, notification of the account activation and the password assigned to the user will be sent to the email address you just entered for the user.
- Click *Save* to create and add the new account to the user list.

When a new user account is created from the New User Registration link, the account is disabled by default, and must be enabled by an administrative user before the new user can log in to Cattrax Web. The User ID name entered by the user requesting an account appears as a new entry in the User List table, but there is no checkmark in the Enabled box for the entry.

To activate the account, an administrative user must highlight the table entry and click the pencil icon to edit the account and open the Edit User dialog box, shown at right. If the account request is accepted, check the *Enabled* square and click *Save*.



The New User Registration link is only displayed on the login page if the Email notification function of Cattrax Web and the account creation at log in function are both enabled through Server Configuration, refer to paragraph 5.13.9.

New users are notified by Email that their account is now active.

Creation of a user account may fail due to any one of these reasons:

1. User ID is not unique – If the user ID is already used by another existing account.

2. Password is invalid – Password must be at least 7 characters long with at least one non-alphanumeric character (!, @, *, etc.)

3. First and Last Name not provided.

4. Password retrieval security question and /or answer not provided.

Reset User Password

Lost passwords cannot be retrieved from the Cattrax Web database. The user account password must be reset and a new password issued by the Cattrax Web application; the user can then change the newly issued password after log in.

User passwords may be reset by either of two possible methods:

- If the function is enabled through server configuration, a user may request a new password through the *Forgot Your Password..?* link on the login page
- An administrative user may reset a users' password through the User List page.

Note that the *Forgot Your Password?* link is only displayed on the login page if the Email notification function of Cattrax Web and the user password reset function are both enabled through Server Configuration, refer to paragraph 5.13.9.

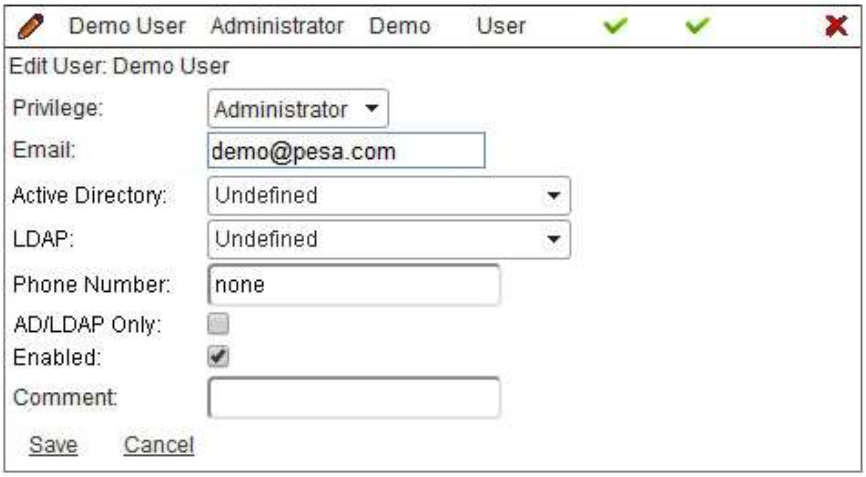
To reset a user password as an administrative user, highlight the User ID entry in the User List table and click the *Reset Password* button beneath the table. You will be prompted to verify the action before the new password is issued.

If the Email notification function of Cattrax Web is enabled, the user is sent their newly created password by Email.

When a user password is changed, Cattrax Web displays the newly created password to the administrative user requesting the change. This will be the only time the password is visibly displayed by Cattrax Web. You should make a notation of the password in the event the Email delivery is not successful, or for paper delivery to the user if a password is reset without Email notification enabled.

Edit User Dialog Box

An administrative user can change privilege level, change contact information for a user, associate the users' account to a network user ID for Active Directory or LDAP alternate login capability, or disable a user account using functions available through the Edit User dialog box, as shown here.



Edit the account of a Cattrax Web user as follows:

- Locate the User ID of the account you wish to edit from the User List and click the pencil icon to the left of the User ID entry. The Edit User dialog box opens beneath the entry row in the User List.
- You may use the drop-down list to select a new privilege level for the user. A Supervisor level user can not assign a user the level of Administrator.
- Make any changes needed to the user Email address information.

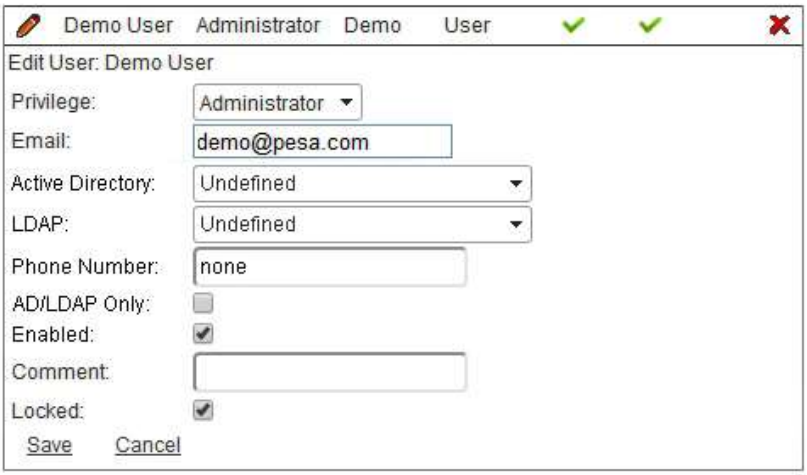
- You may associate the Cattrax Web user's account to a user ID on the facility network for login access through Active Directory or LDAP. Open the drop-down list in the *Active Directory* or *LDAP* field to display a network user ID listing, highlight the desired ID from the list and click. Refer to paragraph 2.2 for more information on alternate login methods.
- Make any changes needed to the Phone Number contact information.
- When checked, the *AD/LDAP Only* checkbox restricts the user to only log in to Cattrax Web through Active Directory or LDAP network server login methods. Placing a check in this box disables the Login Page option of entering application-specific user ID and password credentials assigned to the user at the time of account creation or through subsequent user account changes to access Cattrax Web. Refer to paragraph 2.2 for more information on alternate login methods.
- If you wish to disable the account and deny the user access to the Cattrax Web system, remove the check from the *Enabled* box.
- Make any changes needed to the Comment text.
- Click *Save* to accept the changes to the user account.
- Click *Cancel* to exit the box without any changes to the user account.

User Lockout

If a user fails to login after 5 attempts within 10 minutes, Cattrax Web locks the user's account and the user will not be able to login until an administrative user unlocks it by un-checking the *Locked* checkbox in the Edit User dialog box.

To unlock an account, highlight the locked account and click the pencil icon to open the Edit User dialog box, shown below. Un-check the *Locked* square and click *Save*.

If the Email notification function of Cattrax Web is enabled, the new user is notified by Email that their account is unlocked.



NOTE	1. New User Registration from the Login page is disabled by default, but may be enabled from the Server Configuration page. 2. Both New User Registration and Forgot Your Password..? links are disabled if the administrative Email option is not enabled through the Server Configuration page.

5.7.2 USER PROFILE PAGE

The User Profile page allows the currently logged in user to review, edit and customize user account information and preferences.

A user with access to the Setup home page can open the profile page by clicking the *User Profile* icon. Users of all levels can open the profile page by clicking the user name displayed in the upper right corner of every Cattrax Web page. An example User Profile page is shown by Figure 5-6.

Figure 5-6 User Profile Page

Through the User Profile page, individual users may enter or edit the following personal profile data:

Email, **First Name** and **Last Name** entries are displayed for reference, and can not be modified from this page.

Change Password and Security Question:

The logged-in user may change the password or security question of the account:

- Click the *Change Password* link to open the dialog box as shown at right. Enter the current account password and then enter the new password you wish to create. Confirm the new password and click the *Change Password* button.

- All passwords must be at least 7 characters long with at least one non-alphanumeric character.

- Click the *Change Security Question* link to open the dialog box as shown here, and enter the account password. Enter the new security question you wish to use and enter the answer to the question in the appropriate fields. Click *Save* to complete the change process.

Startup Mode:

The drop-down list allows you to select the Setup home page, the Switching page, or the Event Stack page as your landing page when you login to Cattrax Web.

Startup Workspace:

This drop-down opens to a list of all workspaces to which the logged-in user is authorized access. You may choose a specific workspace to access whenever the Switching page is opened, or you may choose to have the Switching page open with the Last Used Workspace.

Theme:

With the exception of the login page, Cattrax Web gives an individual user the option of choosing a dark or light background theme for all user pages. The choice of background theme used should be based on several possible factors, including ambient lighting conditions in the operator's environment or simply personal preference.

Choose the desired background theme from the drop-down list.

Creation Date, **Last Activity Date**, **Last Login Date** and **Role** of the user are provided for reference.

5.7.3 USER GROUPS

The User Groups page, Figure 5-7, displays the current list of Cattrax Web user groups and the users assigned to each group. Functions available through this page allow an administrative user to create or edit user groups and to add or remove individual users to and from groups.

Any user group entry in the list may be expanded to display the group members by clicking the small right-facing arrow on the left side of the group name entry you wish to open.

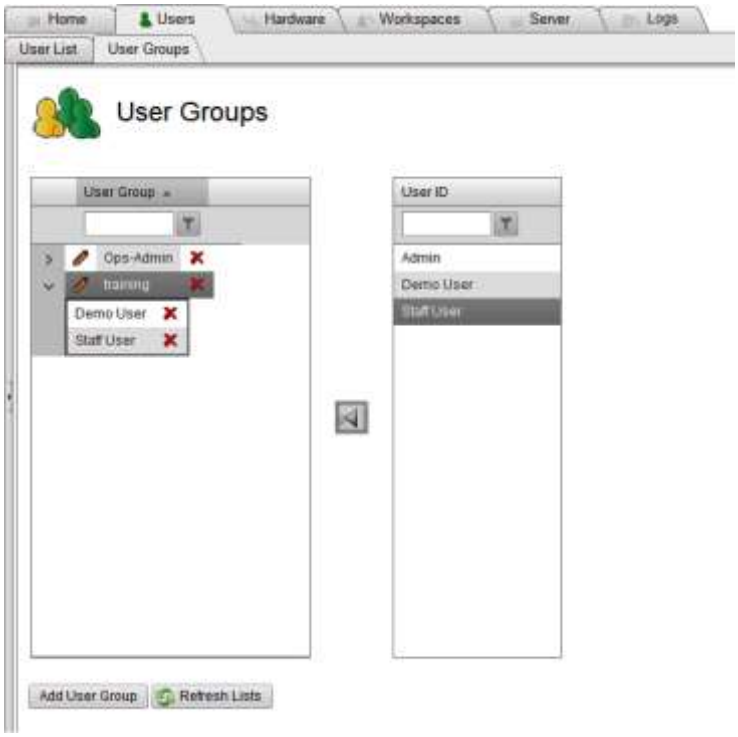


Figure 5-7 User Groups Page

You may add or delete a user group, or edit a user group name as follows:

- Click *Add User Group* to add a new group. A pop-up dialog box prompts you to enter a name for the user group you wish to add, as shown at right.

- Click *Save* to add the new group to the list.
- To delete a user group, click the *red "x"* at the right edge of the group name entry you wish to delete. You will be asked to confirm the action before the group is removed.
- You may change the name of a user group by clicking the *Pencil Icon* to the left of the group name you wish to edit.
- Make any desired changes to the group name and click Sa*ve* to retain the change.
- Click C*ancel* to exit the dialog box with no change.

Individual users may be added to or deleted from a user group as follows:

- Expand the user group entry to display current membership by clicking the right-facing arrow at the left edge of the group name entry you wish to edit.
- Add individual users to the group by locating their User ID in the list on the right hand side of the page. Click the user name and then click the arrow button between the columns to add the User ID to the user group list.
- To delete an individual user from a group, locate the user name in the group membership list and click the *red "x"* at the right edge of the user name entry you wish to delete. You will be asked to confirm the action before the user is removed.

5.8 CATTRAX WEB CONTROL SYSTEM ARCHITECTURE OVERVIEW

The Cattrax Web system consists of a number of virtual components and control elements, created during configuration of the Cattrax Web application, that work together in a hierarchical order to control and limit access by individual users and user groups to specific router system resources. In order for Cattrax Web to function as a control element in conjunction with the PERC2000 or PERC3000 System Controller, there must be a logical association established between the actual hardware controller device and a virtual component of Cattrax Web called a *Virtual Controller*.

In most all PESA installations, a common system controller device (hardware) coordinates operation of the entire router system and all router components. In order for the controller to operate, a router configuration file that controls all aspects of system controller operation is created and loaded into the controller's on-board memory. Among many other things, the router configuration file defines all of the router system resources (signal sources and destinations, switching levels and components, and system salvos). It is the router system resources that allow router control devices (hardware panels or software switching applications such as Cattrax Web) to make signal switches through the router system components.

In order to create a Cattrax Web control instance, the following virtual components must be defined and configured by an administrative user:

Virtual Controller – A Virtual Controller is a named component that associates a virtual control instance to actual PESA system controller hardware in the router installation. Cattrax Web allows multiple virtual controllers in a configuration; all of which may be associated to the same hardware system controller. Router system resources defined by the hardware system controller configuration file are accessible by the virtual control devices of Cattrax Web.

System Resource Include Lists – System Resource Include Lists define the source signals, destination signals, switching levels and *system* salvos that are accessible through the Cattrax Web control instance to which they are associated. These lists are created by selecting specific system resources contained in the router configuration file of the system controller to which a virtual controller is associated.

Subsystem – A Subsystem is a named Cattrax Web component that establishes a logical association between a specific set of system resource include lists and a virtual controller.

Workspace – A Workspace is a named control instance that associates a subsystem to individual users or user groups, and grants these users access to the signal partition of the router defined by the resource include lists associated to the subsystem.

Figure 5-8 illustrates the virtual components of Cattrax Web required to configure a control system instance. The illustration shows two virtual controllers, with two subsystems associated to each; and two workspace elements associated to each subsystem. In an actual configuration, there is no limit to the number of virtual elements allowed by Cattrax Web.

Once users are granted access to a specific workspace either as individual users or by membership in a user group granted access to the workspace, they may control and monitor status of the signal groups, levels and salvos contained in the lists defined for the workspace instance. Control and monitor functions are accessed from the Switching page.

In Cattrax Web architecture, at least one virtual controller must be configured to communicate commands and status between the hardware system controller to which it is associated, and at least one Cattrax Web subsystem must be configured for that virtual controller. For Cattrax Web subsystem configuration purposes, system resources configured for the hardware system controller also become resources available to any virtual controller(s) associated to that hardware controller.

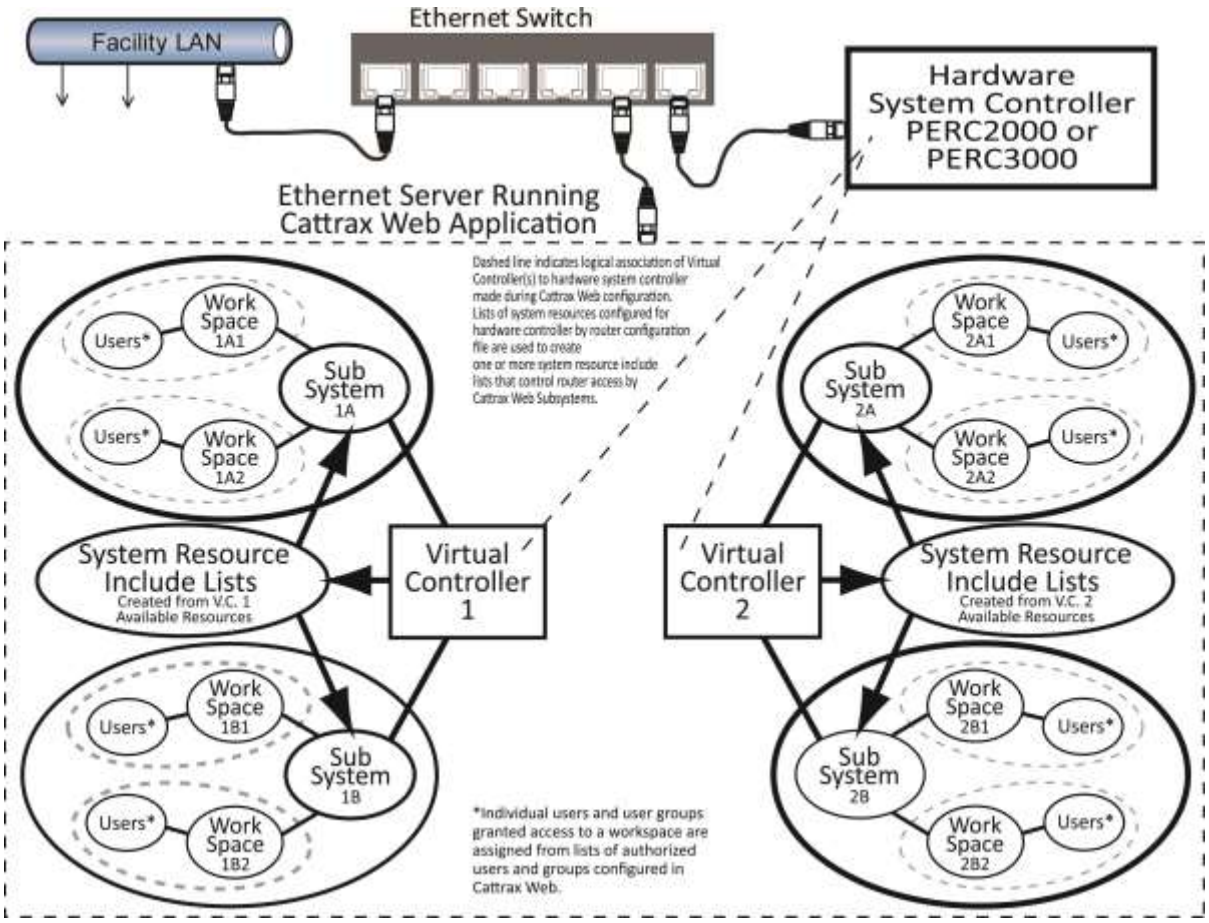


Figure 5-8 Cattrax Web System Diagram

5.9 CATTRAX WEB SYSTEM CONFIGURATION

Configuring a Cattrax Web system consists of creating the various virtual components and workspace assignments for the installation. Once configured, the set-up may be saved as a file and later used to restore the installation, if ever needed.

Here is an overview of the steps required to configure a Cattrax Web control instance:

1. Define one or more Cattrax Web virtual controller instances by name, and associate each one to the actual System Controller hardware. This is done through the **Virtual Controllers** page accessed through the Setup home page.

NOTE	In most installations there is only one hardware system controller and all defined Cattrax Web virtual controllers are associated to the same hardware system controller, but configured to control specific partitions or segments of the overall router installation.

2. Create Lists that define which sources, destinations, switching levels and system salvos under control of the system controller hardware are available to the subsystem. This is done through the **Create Lists** page.

3. Define subsystem instances that associate a set of specific lists to a virtual controller. This is done through the **Subsystems** page.

4. Define which individual users or user groups are granted access to the defined subsystems. This is done through the **Workspaces** page.

For example, assume you are going to grant user access to a number of operator stations in an editing suite and you want to custom tailor each operator station for control access to only the partition of the router that routes signals pertinent to that station. You could define a **virtual controller** named *Edit Suite* and associate it to the router hardware system controller. Then by defining system resource include **lists** and **subsystems** for the virtual controller named Edit Suite and configuring **workspace** assignments for particular users, or groups of users, you can designate and limit access to the router in virtually any way you wish. Likewise, in the same installation, if you wish to grant entirely different access capability to the engineering group, you could define a virtual controller named *Engineering*. This Cattrax Web component associates to the same hardware system controller, but now it allows you to configure lists, subsystems and workspace assignments for completely different router access. The tiered **Virtual Controller → Lists → Subsystem → Workspace** user configuration scheme allows a great deal of flexibility in planning your router control operation. When an authorized user logs in to Cattrax Web and opens the Switching page, the user configuration specifically defines the workspaces that an individual user can view and control.

5.10 HARDWARE CONFIGURATION PAGES

Virtual Controllers, Resource Include Lists and Subsystems are created through the Hardware Configuration pages of Cattrax Web. These pages may be accessed from either the Setup home page icons or by clicking the *Hardware* tab in the menu bar.

5.10.1 CONTROLLERS PAGE

The Controllers page, Figure 5-9, lists PESA hardware system controllers discovered on the device network by name and IP address. In most installations only one system controller device is used and would be the only device listed in the display. The Status column identifies the offline or online status of the system controller device. Click on a controller device entry to select and highlight the table row. A separate box, to the right of the Controller list, identifies the network operating parameters of the selected device.

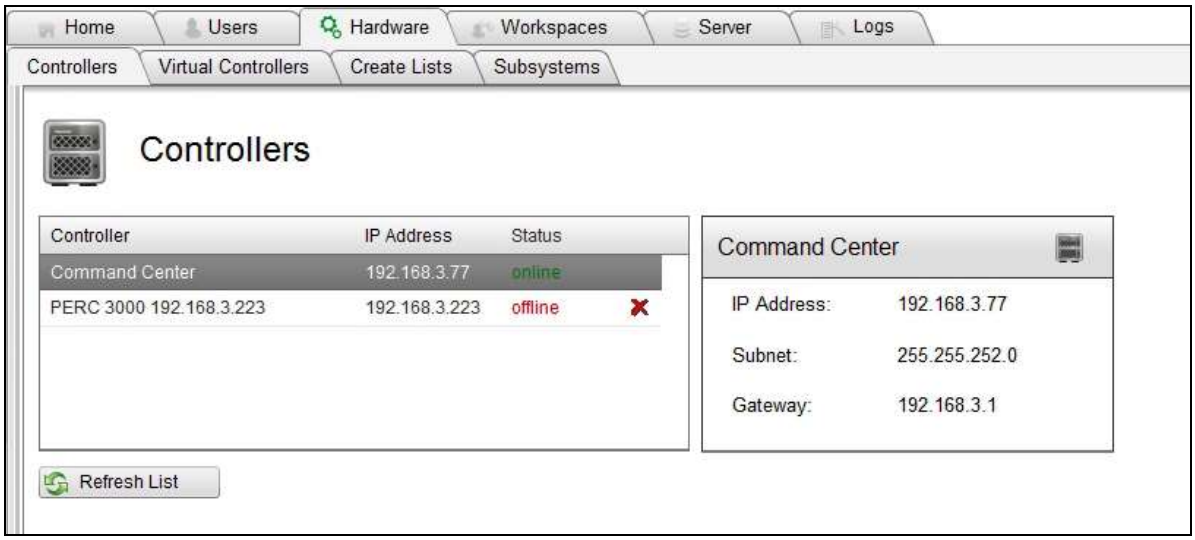


Figure 5-9 Controllers Page

If a hardware controller is offline, any virtual controller(s) associated to the device cannot actively control the router. You may assign the same hardware system controller device to any number of different Cattrax Web virtual controllers.

5.10.2 VIRTUAL CONTROLLERS PAGE

The Virtual Controllers page allows you to add, edit and delete Cattrax Web virtual controller components. A virtual controller must have a unique name and be associated to a system controller device that has been discovered by Cattrax Web. You may associate the same hardware controller to any number of different Cattrax Web virtual controllers. An example Virtual Controllers page is shown by Figure 5-10.

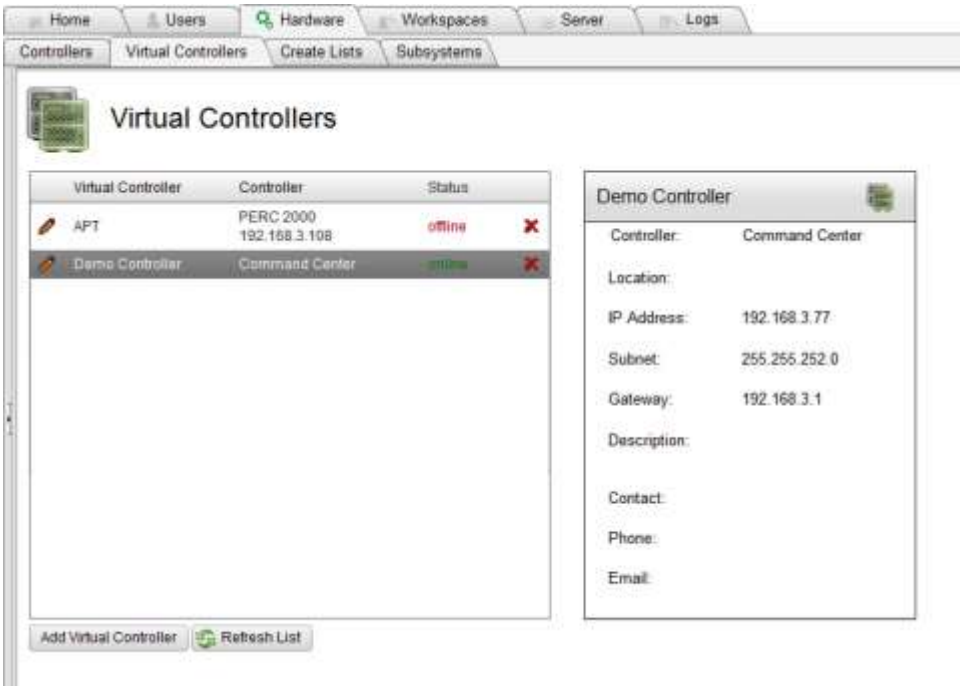


Figure 5-10 Virtual Controllers Page

You may add or delete a virtual controller, or edit a controller name as follows:

- Click the *Add Virtual Controller* button to add a new controller component and open the pop-up dialog box, as shown here.
- Enter a name for the new virtual controller in the box beside the prompt.
- The Status entry line contains a drop-down listing of all available hardware system controller devices in the router installation, and displays the current online/offline status of each device. In most installations there will only be one device listed.

- Select the system controller device from the listing that you wish to associate to the virtual controller you are creating.
- The remaining entries: Location, Contact, Phone, Email and Description are free text entry areas that you may use to further define the component you are creating. It is not necessary that data be supplied in any of these areas in order to create the virtual controller and add its name to the table listing.
- Click the *Save* button to add the new virtual controller to the table.
- To delete a virtual controller, click the *red "x"* at the right edge of the name entry you wish to delete. You will be asked to confirm the action before the component is removed.
- You may edit the name or other information of a virtual controller by clicking the *Pencil Icon* to the left of the name you wish to edit.
- Make any desired changes to the name or other data in the dialog box and click *Save* to retain the change.
- Click C*ancel* to exit the dialog box with no change.

NOTE	1. If the hardware system controller used by a Cattrax Web virtual controller is changed through the Virtual Controllers page, the resource include lists created for the Virtual controller will be deleted. 2. If a virtual controller is deleted all subsystems and workspaces associated to it are also deleted.

5.10.3 CREATE SYSTEM RESOURCE INCLUDE LISTS

The Create Lists page allows you to create named System Resource Include Lists that identify system resources, by resource type, to which you wish to allow control and status access by Cattrax Web subsystem components configured for a specific virtual controller. Individual lists may be created for Sources, Destinations, Switching Levels and System Salvos from listings of all system resources available through the virtual controller to which the list is associated. You may create lists that grant signal access and control groupings for certain users or user groups, specific programming requirements, or any number of other applications.

If you are familiar with the steps to create a router configuration file through PESA's Cattrax application, the lists we create for a Cattrax Web subsystem are very similar in purpose to the Panel Key Lists that you create and assign to a hardware control panel, in that panel key lists specify the system resources the panel is authorized to control.

Each list you create is assigned a unique name and may be populated with some or all entries of the list type contained in the configuration file of the hardware system controller associated to the specified virtual controller. There are four list types:

Sources – Contains a listing of router sources included in the list.

Destinations – Contains a listing of router destinations included in the list.

Levels – Identifies router switching levels for which this list grants control.

Salvos – Identifies the *system* salvos included for operator access through this list.

As a method of further designating and limiting access to the router, multiple lists of each system resource type may be created from the set of resources identified for a virtual controller, and access to each list may be granted or denied as desired to the various subsystems created under the virtual controller.

An example Create Lists page is shown by Figure 5-11.

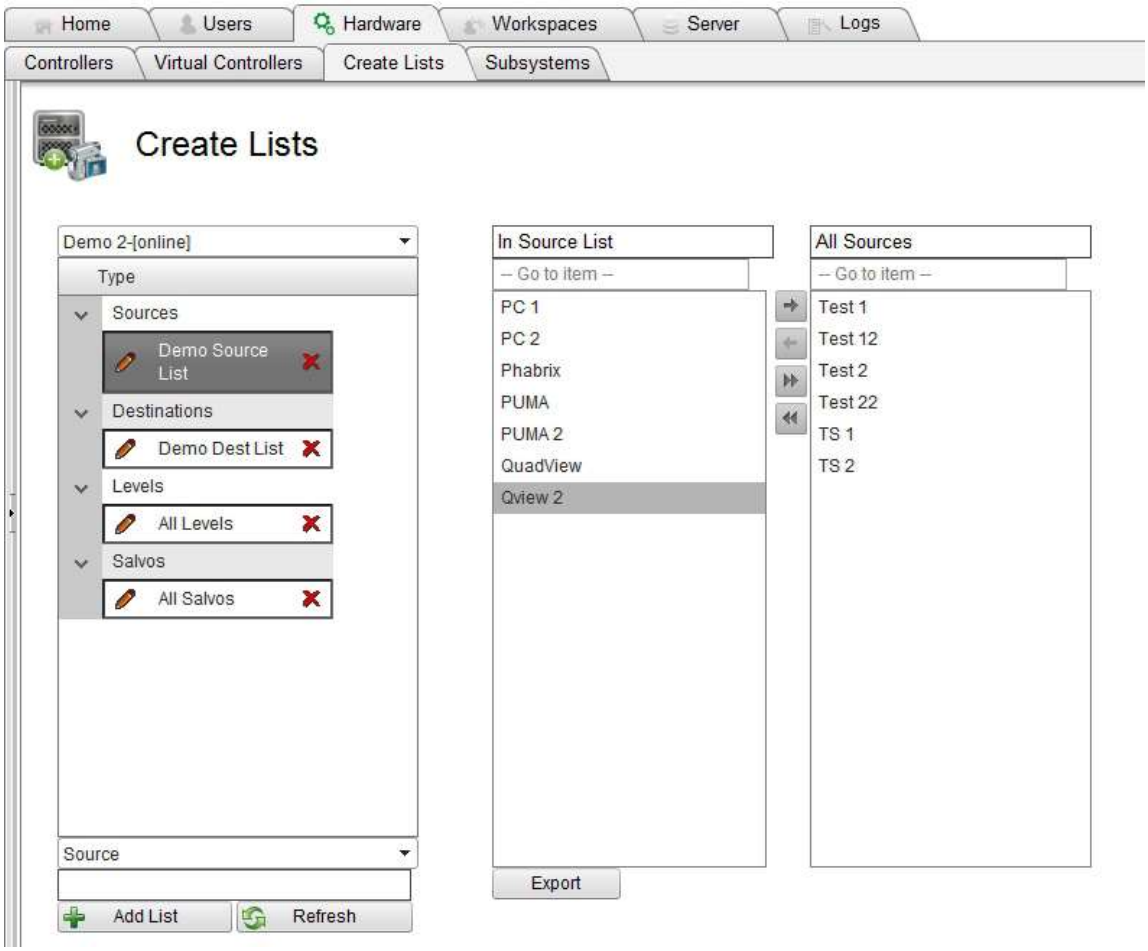


Figure 5-11 Create Lists Page

There is a drop-down menu at the top of the column on the left that opens to a list of all virtual controllers configured for Cattrax Web, refer to Figure 5-12. Beneath the virtual controller field is a table where each of the four system resource list types are displayed with an arrow icon to the left of each entry that expands the listing contents. When a list type entry is expanded, any lists already created for the system resource type, are identified under the header.

To the right of the table are two columns, labeled *In <list type> List* and *All <available list type entries>*.

In xxx List displays the contents of a list selected from the table.

All xxx displays the available signals, levels or salvos contained in the hardware system controller's configuration file that have not been included in the content of the list.

Create Lists Page Configuration

You may add and populate lists associated to a virtual controller as follows:

- Open the *Virtual Controller* drop-down menu, as shown in Figure 5-12, and select the virtual controller you wish to associate with the resource lists you are creating.

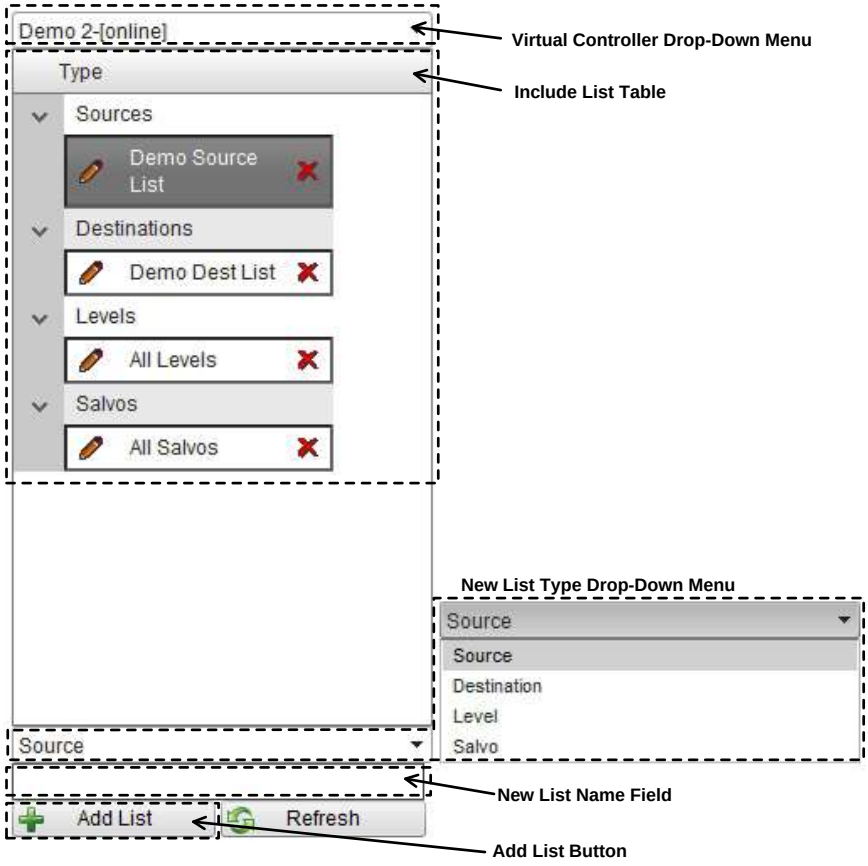


Figure 5-12 Create Lists Configuration

- Select the resource list type you want to create from the drop-down menu beneath the table as shown in Figure 5-12.
- Enter a name for the list in the *New List Name* field and click the *Add List* button to create the new list.
- Locate the list you just created by name under the *Type* entry in the table, and click to select and highlight the entry.
- Initially, there will be no items included in the *In List* column, and all system resources of the selected type available through the virtual controller you selected are displayed in the *All xxx* column.
- Using the arrows located between the column lists, select and move the items you want to add from the available to the included list.
- The list is automatically saved as items are entered to the *In List* column.

You may edit existing lists associated to a virtual controller as follows:

- Open the *Virtual Controller* drop-down menu, as shown in Figure 5-12, and select the virtual controller associated with the list you want to edit.
- Expand the proper resource list type entry in the table and locate the list by name.
- Click the list name to select and highlight the entry.
- All items of the list type currently contained in the list are displayed in the *In List* column, and all entries available for the list type are displayed in the *All xxx* column.
- Using the arrows located between the column lists, select and move items you want to add to the list from the available column to the *In List* column.
- Select and move items you want to remove from the list from the *In List* column to the available column.
- The list is automatically saved as items are moved between columns.

You may change the name of an existing resource list associated to a virtual controller as follows:

- Open the *Virtual Controller* drop-down menu, as shown in Figure 5-12, and select the virtual controller associated with the list name you want to change.
- Expand the proper list type entry in the table and locate the list by name.
- Click the *Pencil Icon* to the left of the list name you wish to change and open the name change dialog box.
- Make any desired changes to the list name in the dialog box and click Sa*ve* to retain the change.
- Click C*ancel* to exit the dialog box with no change.

You may delete existing lists associated to a virtual controller as follows:

- Open the *Virtual Controller* drop-down menu, as shown in Figure 5-12, and select the virtual controller associated with the list you want to delete.
- Expand the proper list type entry in the table and locate the list by name.
- Click the list name to select and highlight the entry.
- Click the *red "X"* at the right edge of the table entry to delete the list.
- You will be prompted to verify the action.

NOTE	If the hardware system controller used by a Cattrax Web virtual controller is changed through the Virtual Controllers page, the resource include lists created for the virtual controller will be deleted.

5.10.4 SUBSYSTEMS

The Subsystems page allows subsystems associated to a virtual controller to be created, configured and deleted. In Cattrax Web architecture, a subsystem is a named virtual component that associates resource lists to a virtual controller, thereby configuring the sources, destinations, switching levels and system salvos of the router available through the subsystem to users and user groups authorized to access the subsystem component. Remember that every subsystem must be associated to one, and only one, virtual controller; however, each virtual controller component can have an association with multiple subsystems. Multiple lists of each system resource type may be created and individually assigned to a particular subsystem as a method of designating and limiting access to the router.

Cattrax Web displays the lists associated to a virtual controller system and, through the Subsystem page, allows you to select the list or lists that contain the control assignments you wish to grant to particular users or user groups assigned access to the subsystem. An example Subsystem page is shown by Figure 5-13.

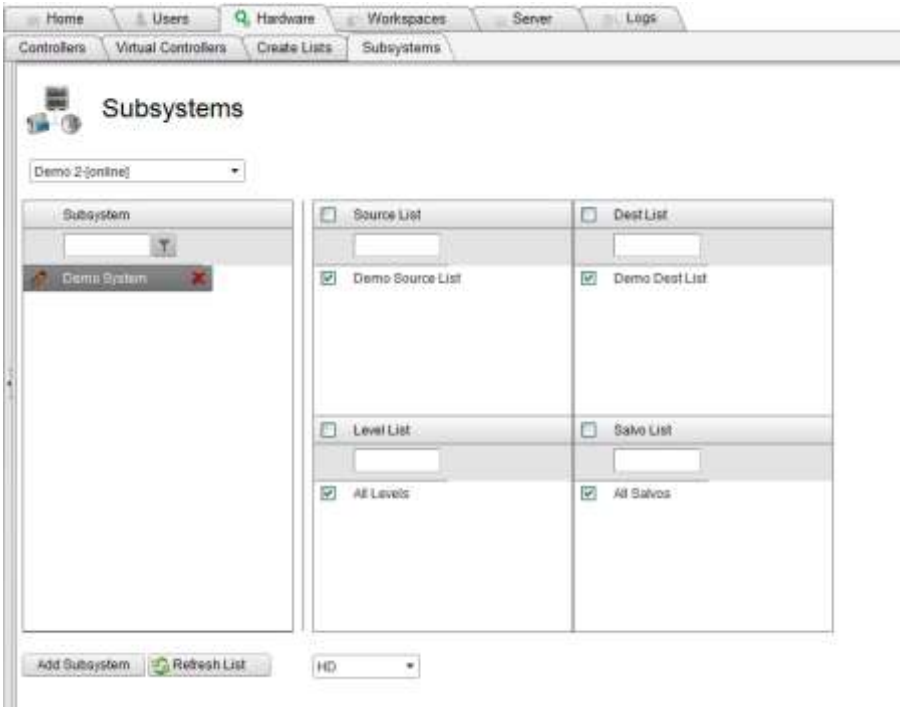


Figure 5-13 Subsystems Page

Above the Subsystem table area is a drop-down menu that opens to a listing all Cattrax Web virtual controllers that have been created through the Virtual Controllers page. When a virtual controller is selected from the list, subsystems that are already defined and associated to that virtual controller are displayed in the Subsystem table. All resource include lists associated to the selected virtual controller are displayed, by type, in the boxes to the right of the subsystem table.

A check mark in the box beside any of the list entries indicates that all system resources included in that list are available to all users granted access to the subsystem currently selected in the Subsystem table.

Configuration of a subsystem involves selecting the Cattrax Web virtual controller from the drop-down menu to which you wish to associate the subsystem, and selecting the list(s) of each type from the displayed available lists for which you wish to grant status and control access to users assigned to the subsystem.

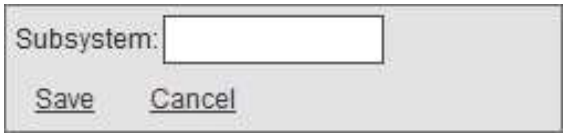
Beneath the Level List display box is a drop-down that lists all the system switching levels available for access by the active (check in the box) level resource lists. The level name displayed in the box is the *Status Level* of the subsystem. Status level indicates the default switching level displayed or controlled by Cattrax Web when the Switching page is displayed in hide level display mode.

Subsystem Page Configuration

Click any subsystem entry in the table to display the lists associated to the subsystem. You may add or delete lists for the displayed subsystem simply by checking or un-checking the box next to each list entry. Checking or un-checking the box in any table header selects or deselects all lists in the table. The default status level may be changed by opening the drop-down list and selecting the switching level you wish to promote to status level. Added or deleted lists or status level changes are immediately updated for the subsystem entry.

You may add or delete a subsystem, or edit a subsystem name as follows:

- Open the drop-down menu and select the virtual controller that you wish to associate with the subsystem you are creating.
- Click *Add Subsystem* to add a new subsystem. A pop-up dialog box prompts you to enter a name for the subsystem you wish to add, as shown at right.



- Click *Save* to add the new subsystem to the list.
- To delete a subsystem, click the *red "x"* at the right edge of the name entry you wish to delete. You will be asked to confirm the action before the subsystem is removed.
- You may change the name of a subsystem by clicking the *Pencil Icon* to the left of the name entry you wish to edit.
- Make any desired changes to the subsystem name and click Sa*ve* to retain the change.
- Click C*ancel* to exit the dialog box with no change.

When a new subsystem is created there are no system resource include lists selected for it. Assign router access to the subsystem as follows:

- Add lists from any of the list groupings to the subsystem by placing a check in the box next to the lists you wish to add to the subsystem. To add all lists in the grouping, check the box in the list group header. You may remove any list from the subsystem by removing the check in the box next to the list entry.
- Open the status level drop-down menu and select the default status level for the subsystem.

NOTE	If a subsystem is deleted all the workspaces associated to that subsystem are also deleted.

5.11 WORKSPACES CONFIGURATION

A **workspace** maps subsystems to individual users or user groups that are given router control access through that subsystem. The Workspaces page allows workspace entries to be created, configured and deleted. Each workspace entry is given a unique name and may only be associated to one subsystem; however, any subsystem may be associated to any number of workspaces. Access the Workspaces user interface page from the Setup home page icon or by clicking the Workspaces tab on the menu bar. An example Workspaces page is shown by Figure 5-14.

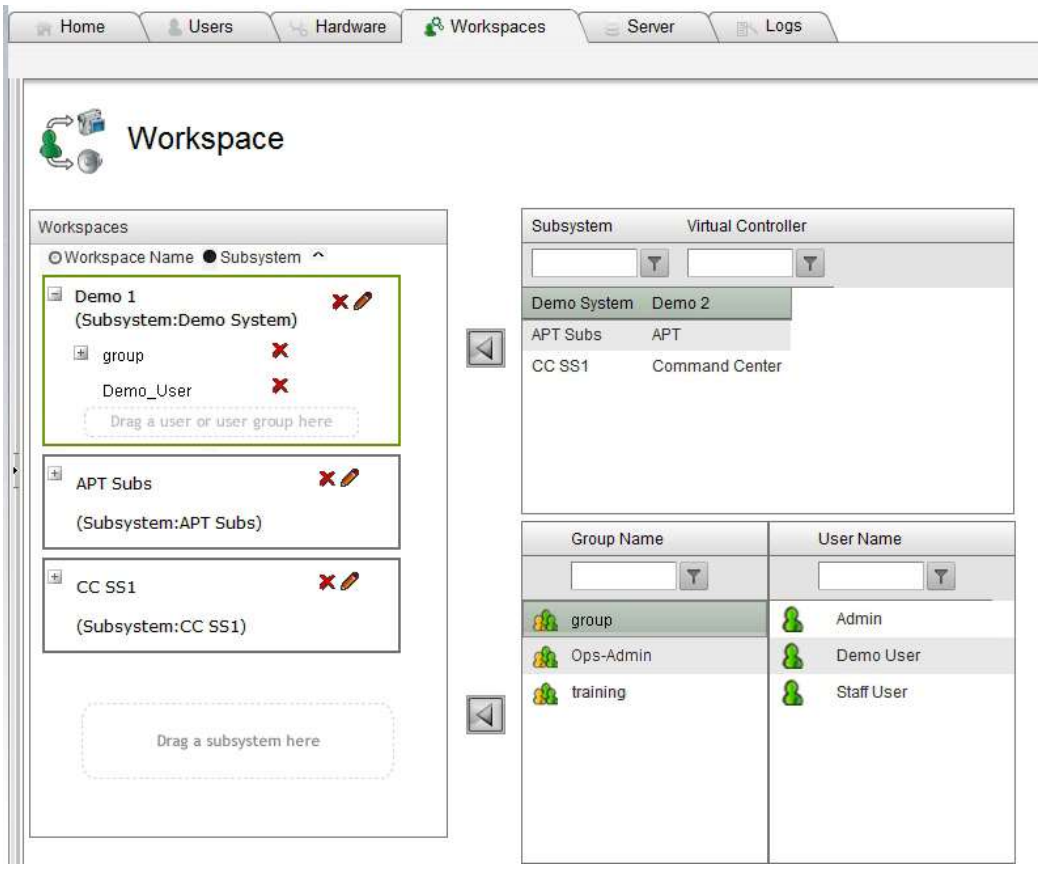


Figure 5-14 Workspaces Page

The Workspaces page displays a listing of all currently configured workspace entries on the left side of the page (Workspaces table). On the right side of the page is an area labeled *Subsystem* that displays a listing of all configured subsystems and also identifies the Cattrax Web virtual controller to which each subsystem is associated.

Beneath the subsystem display is a listing of User Groups (Group Name table) on the left and individual Users (User Name table) on the right.

Each workspace entry is displayed as an individual box in the Workspace table. The name of the workspace is displayed at the top of each box and directly beneath the name in parentheses is the subsystem name associated with the workspace. When a workspace entry is selected from the table, the border of the box is displayed in green. Expanding the workspace entry reveals a listing of all individual users and user groups authorized access to the workspace, as shown by the workspace entry named Demo System in Figure 5-14.

The example workspace entry in Figure 5-14 provides the following information:

- The selected workspace is named *Demo 1*.
- Demo 1 is associated to the subsystem *Demo System*.
- The *Subsystem* table indicates that subsystem Demo System is associated to the Cattrax Web virtual controller named *Demo 2*.
- There is one individual user, *Demo_User*, and one user group, named *group*, granted access to subsystem Demo System through the workspace named Demo 1. You may expand the user group entry to open a list of users assigned to the group.

Whenever the individual user, *Demo_User*, or any member of the user group logs in to Cattrax Web and opens the Switching page through their browser, the workspace *Demo 1* is included in a listing, along with any other workspaces to which they are assigned, from a drop-down menu on the Switching page. By selecting Demo 1 as the active workspace, all router access granted by the lists selected for subsystem Demo System is available to the user from the web browser page. Refer to paragraph 5-17 for more information on the Switching page.

Workspaces Page Configuration

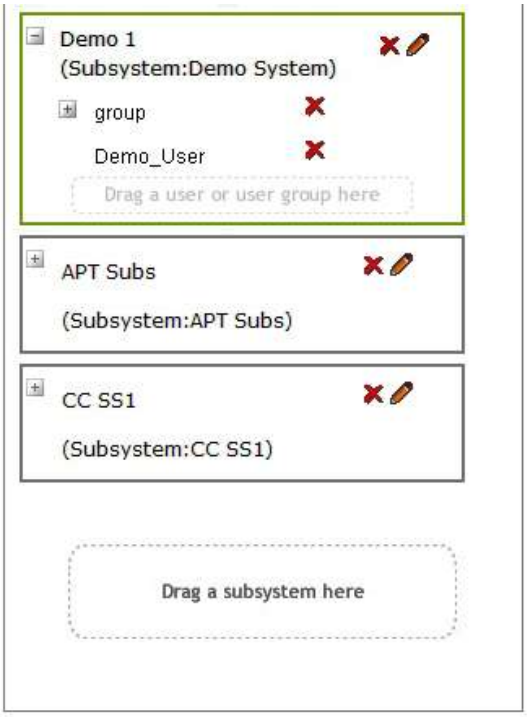
Workspace entries may be added and associated to a subsystem by either of two methods:

Method 1

- Click on the subsystem name in the table on the right side of the page for which you wish to create a new workspace.
- Click the top left-facing arrow between the listing areas to add the name to the Workspaces table.

Method 2

- Scroll to the bottom of the workspace list area and locate the box labeled "*Drag a subsystem here*", as shown at right.
- Locate the subsystem you wish to associate with the workspace you are creating from the Subsystem table on the right side of the page.
- Left click, hold and drag the subsystem name to the "*Drag a subsystem here*" box.
- A new workspace entry is added to the listing.



Regardless of which method you use to add a new workspace, the following steps complete the process:

- By default, the subsystem name is entered as the workspace name until the name is changed as desired.
- Click the *Pencil Icon* to the right of the name entry and enter a name for the new workspace in the pop-up dialog box and click Sa*v*e to retain the change.

- Assign users to the new workspace by either of the two methods discussed in the next paragraph.
- To delete a workspace entry, click the *red "x"* just to the right of the workspace entry name you wish to delete. You will be asked to confirm the action before the workspace is removed.

Click any workspace entry in the table to display the subsystem and users configured for the workspace. Ensure that the border around the workspace you clicked is shaded green. You may add individual users or user groups to the workspace by either of two methods:

Method 1

- Click on the user name or the group name in the appropriate table on the right side of the page that you wish to add to the workspace.
- Click the bottom left-facing arrow between the table areas to add the name to the workspace listing.

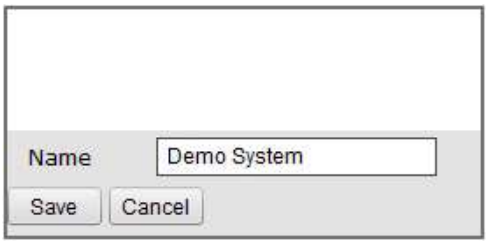
Method 2

- Left click, hold and drag the user name or group name you wish to add to the workspace to the box labeled "*Drag a user or user group here*" at the bottom of the workspace entry.

To delete users or user groups from the workspace click the *red "x"* at the right edge of the name entry you wish to delete.

You may edit or change a workspace name or delete a workspace entry as follows:

- Click the *Pencil Icon* to the right of the workspace name entry you wish to edit. A pop-up dialog box displays the current name, as shown here.
- Make any desired changes to the workspace name and click Sa*ve* to retain the change.
- Click C*ancel* to exit the dialog box with no change.



- To delete a workspace entry, click the *red "x"* just to the right of the workspace entry name you wish to delete. You will be asked to confirm the action before the workspace is removed.

NOTE	1. If the hardware system controller used by a Cattrax Web virtual controller is changed through the Virtual Controllers page, the resource include lists created for the virtual controller will be deleted. 2. If a virtual controller is deleted all subsystems and workspaces associated to that virtual controller are also deleted. 3. If a subsystem is deleted all the workspaces associated to that subsystem are also deleted.

5.12 SERVER CONFIGURATION FUNCTIONS

Functions available through the Cattrax Web Server Configuration page allow system administrator level users to manage and maintain the server. Server pages are accessible only to users with administrator privileges, with the exception of the Logs page which is accessible to both administrator and supervisor level users. Access Server Configuration functions from the Setup home page icon or by clicking the *Server* tab on the menu bar.

5.13 SERVER CONFIGURATION USER INTERFACE PAGE

The Server Configuration page, Figure 5-15, provides a user with administrator privileges access to a collection of system configuration functions and options. Each functional area of the page is discussed in the following paragraphs.

Figure 5-15 Server Configuration Functions and User Interface Page

5.13.1 SUBNET BROADCAST ADDRESS CONFIGURATION (SUBNET INFORMATION)

Refer to paragraph 5.5.

5.13.2 SYSTEM RESOURCE ICONS (DISPLAY OPTIONS)

Cattrax Web allows you to optionally place a user selectable icon next to system resource listings (sources, destinations and salvos) on the switching page, event stack page and schedule editing page, if desired. Check the box next to the *Show Icons for Source/Dest/Salvos* entry to activate the show icons option. When icons are used on the display pages, each line entry will use twice the page space as text only listings.

NOTE	Graphical icons are not created through Cattrax Web. Icons you wish you use on the switching display pages must be obtained or created from a source external to Cattrax Web, must be of the proper size and format for Cattrax Web to display, and must be stored on the server hosting the Cattrax Web application, as discussed in the paragraph below.

Icons for sources, destinations and salvos need to be uploaded to the web server. Place the files in the directory C:\inetpub\wwwroot\Application\Control*type* where *type* is “Source”, “Dest” or “Salvo”. Cattrax Web installs several sample icons. The filename should exactly match the name of the source, destination or salvo it should be associated with and have a file extension of “png”, “gif”, “jpg”, “jpeg” or “bmp”. If the source, destination or salvo name has a character that is not allowed in a filename, it should be replaced with a “-“. Characters not allowed in a file name are “/”, “\”, “<”, “.”, “:”, “|”, “?”, “*” and the double quote character.

5.13.3 SWITCHING OR ROUTING DISPLAY PREFERENCE (DISPLAY OPTIONS)

Cattrax Web allows you to choose between the words “Switching” or “Routing” as the displayed word on all system pages pertaining to switching/routing functions. Check the box next to the *Change the word “Switching” to “Routing”* entry to display the word “routing” rather than the factory default word “switching”. Removing the check will cause Cattrax Web to use the word “switching” on all pertinent system pages.

5.13.4 SYSTEM BROADCAST ANNOUNCEMENT CONFIGURATION (DISPLAY OPTIONS)

Cattrax Web allows you to place a broadcast message in either the header or footer, or both locations, of every user interface page. This message is visible to users of any privilege level. To add an announcement message, check the box labeled *Display system announcement in header* or check the box labeled *Display system announcement in footer*. If you want the message to appear at both the top and bottom of the page, place a check in both boxes. Enter the text you wish to display in the system announcement field. To remove a message, uncheck the appropriate box in the *Display Options* configuration area.

5.13.5 CUSTOM LOGO CONFIGURATION (DISPLAY OPTIONS)

Cattrax Web allows you to display a custom header image at the top of every user interface page in place of the factory default logos. In order to fit the area, the custom image file should be 600 pixels wide by 65 pixels tall. Valid file formats are .png, .jpg and .jpeg.

To add a custom header, click the Custom Logo *Select* box in the *Display Options* configuration area, browse to the image file and click Upload. The PESA default logo header may be restored at any time by clicking the *Restore Default Logo* button.

5.13.6 GENERAL SETTINGS

The drop-down list labeled ***Theme*** allows you to choose a dark or light background theme for the login page of Cattrax Web. This setting selects only the login page background and does not override an individual users' display theme setting for all other browser pages made through the User Profile page.

Update Interval allows you set the rate at which browser pages are refreshed by the server running Cattrax Web. From the drop-down list, you may choose a refresh rate of 1 to 4 seconds. The default is 1 second, and this setting should always be used unless you are experiencing slow performance issues with the server.

Log Level allows you choose the detail level at which log data is written to the xxx.ctx file used for system troubleshooting. The .ctx file is automatically created by Cattrax Web and stored by the server running the application. This file is rarely, if ever, accessed or open by a user of Cattrax Web during normal operation of the application, and is accessible only by opening the program folder where the file is stored. If it is ever necessary to troubleshoot the Cattrax Web system, a PESA Customer Service technician may ask you to access this file. Factory default for the log level is *Debug*, and should not be changed unless requested by a PESA technician. If it is ever necessary, you may select the log level from the drop-down list options shown at right.

5.13.7 CONTACT INFORMATION ON LOGIN PAGE

You may choose to display an Email address and/or a telephone number in the login dialog box that allows users to contact a system administrator. Simply enter the Email address and phone number in the appropriate fields. Data present in either of these fields is displayed in the lower portion of the login dialog box.

5.13.8 ADMINISTRATIVE EMAIL COMMUNICATION SETUP

Cattrax Web includes an Email server function that allows the application to communicate with registered users through the facility Email system. Activate the Email server function by placing a check in the box labeled *Allow administrative email communication* and enter the address of a SMTP mail server and a username and password for an email account on that server. In the *From* field, enter the name you wish to appear as the from address on email sent by Cattrax Web. Enter the port number of the SMTP mail server. Check the *"Use SSL"* box if email should be sent using SSL.

Email notifications sent to the Cattrax Web system, such as notification of a new user request or user password change request from the login page, are sent to the email address entered on the User Profile page for the default ***Admin*** user.

5.13.9 USER INACTIVITY TIMER CONFIGURATION (SECURITY SETTINGS)

The inactivity timer function of Cattrax Web checks each logged in user for interface activity with the application and compares periods of user inactivity against the number of minutes configured for timeout. When a user is inactive for the specified number of minutes, the account becomes inactive and in order to continue with any session activity, the user is redirected to the login page, and must re-enter the User ID and Password of the account. Enter the number of minutes you wish to allow before timeout in the field.

NOTE	**A logged-in user continues to count against the number of users allowed by the license until one of the following occurs: a) the timeout expires, b) the user logs out, c) Cattrax Web is restarted. Cattrax Web cannot detect that a browser tab or window has been closed and so cannot reduce the active user count when this happens. Setting this timeout to a large value, combined with users not explicitly logging out, could cause all the available users' slots to be considered taken even though there are perhaps only a few actual simultaneous users.**

5.13.10 LOGIN DIALOG BOX USER PROMPT CONFIGURATION (SECURITY SETTINGS)

Cattrax Web can display prompts in the login dialog box that allow a new user to create a user account and request activation directly from the browser page, or allow an existing user to change their password. An administrative user can select either or both of these prompts for display by checking or un-checking the appropriate box in the user prompt configuration area. In order for either of the prompts to display, regardless of whether the box is checked, the System Email function must be enabled and configured as a valid Email account for the facility.

5.13.11 ALTERNATIVE LOGIN CONFIGURATION (ACTIVE DIRECTORY & LDAP)

Refer to paragraph 5.14.

5.13.12 ERROR MODE (ERROR MESSAGES MODE)

Cattrax Web can display reported server errors which may be useful in system troubleshooting, if necessary. The Error Mode list allows you to set how network server errors are displayed from the following options:

- **Server Only** – Displays server errors only on the server machine hosting the Cattrax Web application.
- **Always** – Displays server errors on all open instances of Cattrax Web.
- **Never** – Server errors will not be shown by Cattrax Web.

5.14 ALTERNATIVE LOG-IN CONFIGURATION (OPTIONALLY AVAILABLE FEATURE)

The following configuration steps are only required if your Cattrax Web installation is licensed to use alternative log-in options.

Cattrax Cattrax Web supports two methods of user log in with externally authenticated domain login credentials through an external server running the Lightweight Directory Access Protocol (LDAP) such as Microsoft Active Directory Domain Services (AD).

The first is by entering the username and password for the external service that uses LDAP. The second, available only when using AD, uses NT LAN Manager (NTLM) along with LDAP and does not require a username or password to be entered, but instead uses the credentials used to log on to the Windows domain.

A functional tutorial on the network/IT requirements for these services is beyond the scope of this User Guide. The setup and configuration settings you enter through Cattrax Web provide the interface links and operational data to these external network services.

If you, as the Cattrax Web administrator performing this system setup step are not familiar with the setup and operational requirements of the AD or LDAP services, PESA highly recommends that you consult your IT support staff, facility network administrator or other resource knowledgeable of these external services for assistance before proceeding.

In order to use either of these methods, you must first configure Cattrax Web through settings entered in the fields on the Server Configuration page. Each field is introduced in the following paragraphs.

Configure Cattrax Web for use with an LDAP service as follows:

- **Show button to login with LDAP using name/password** – A check in this box authorizes external credential logins to Cattrax Web with LDAP. The LDAP login button will be shown on the login page to allow a user to login using external credentials by entering their username and password.
- **LDAP Friendly Name** - This is a free text field that allows you to enter the text label that will be displayed to users on the Cattrax Web login page in the button used to launch an LDAP login. The text "LDAP" is the factory default, but you may change the button label to a more descriptive or localized prompt, if desired.
- **Allow users to login with LDAP using NTLM** – A check in this box authorizes external credential logins to Cattrax Web with LDAP using NTLM. The NTLM login button will be shown on the login page to allow a user to login using external credentials without entering their username and password. The credentials used to log on to the Windows domain will automatically be used.
- **NTLM Friendly Name** - This is a free text field that allows you to enter the text label that will be displayed to users on the Cattrax Web login page in the button used to launch an LDAP with NTLM login. The text "Active Directory" is the factory default, but you may change the button label to a more descriptive or localized prompt, if desired.

The following fields apply to both types of logins:

- **Server** - Enter the address and port number of the LDAP server in this field. The default field entry is the address of the web server currently hosting the computer running Cattrax Web.
- **Base Distinguished Name** – Enter the proper series of Relative Distinguished Names, separated by commas, which define the directory entry from which searches occur.
- **Format - Filter** – Using LDAP protocol syntax; enter a filter that will be used to filter the results of the search.
- **Format - Display** – Using LDAP protocol syntax; enter the formatting commands to set the format of the display name that will be sent to Cattrax Web from the LDAP server.
- **Format - Login** – Using LDAP protocol syntax; enter the formatting commands to set the format of the login name that will be sent by Cattrax Web to the LDAP server.
- **Format – User ID** – Using LDAP protocol syntax; enter the formatting commands to set the format of the text that will be used as the User's login ID.
- **User - Name** – If required by your network configuration, enter the User Name that Cattrax Web uses to login to the LDAP server.
- **User - Password** – If required by your network configuration, enter the Password that Cattrax Web uses to login to the LDAP server.
- **User – Domain** – If required by your network configuration, enter the name of the network domain in which Cattrax Web resides.

5.15 BACKUP & RESTORE

Through the Backup and Restore page, Figure 5-16, it is possible to backup and restore the Cattrax Web database. Backup database files are stored on the system server. Click *Backup Database* to write the current database to the server. The file is added to the Backed-Up Database List, as shown. If you ever need to restore Cattrax Web to a particular database, simply select the desired database filename from the listing and click the *Restore Database* button.

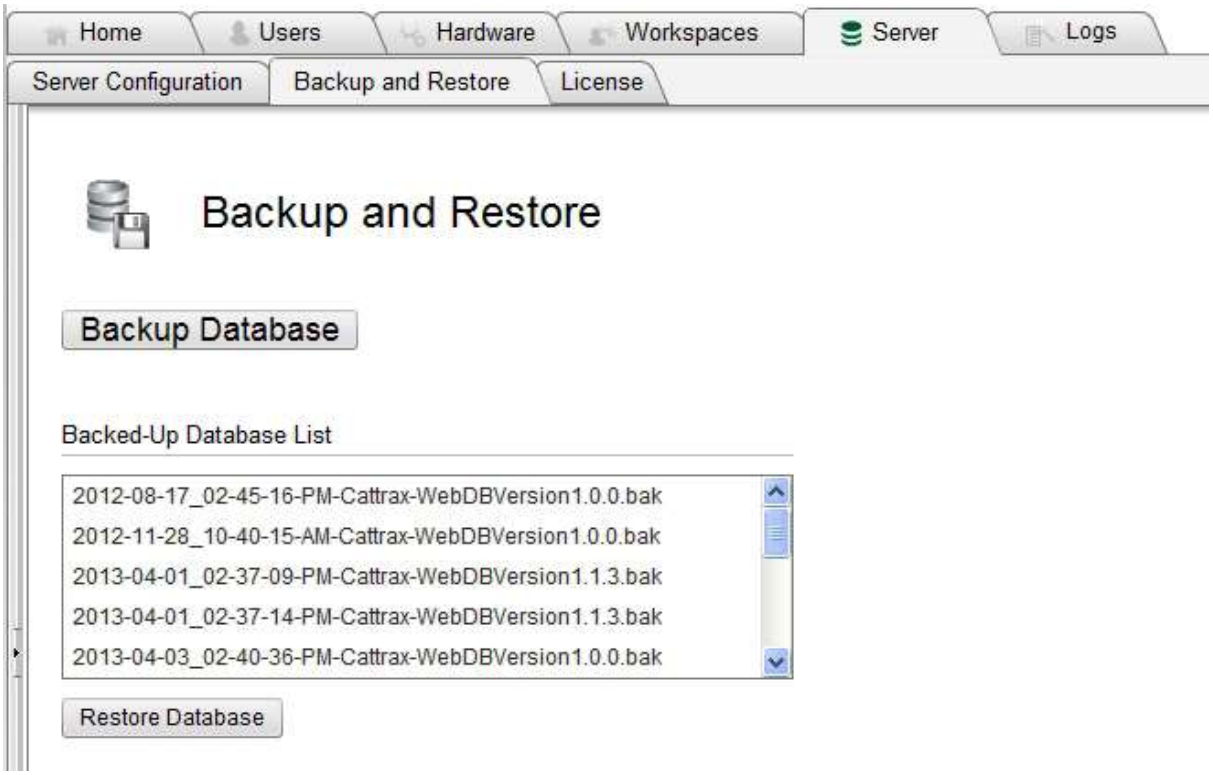


Figure 5-16 Backup and Restore Page

NOTE	Database version number is added to the database backup files. The backup version must match the current active database version when restoring, otherwise it will be rejected by Cattrax.

5.16 LICENSE

Refer to paragraph 4.2.

5.17 LOGS

Through the Logs page, administrators may view the events and error logs maintained by Cattrax Web in chronological order. An example Logs page is shown by Figure 5-17.

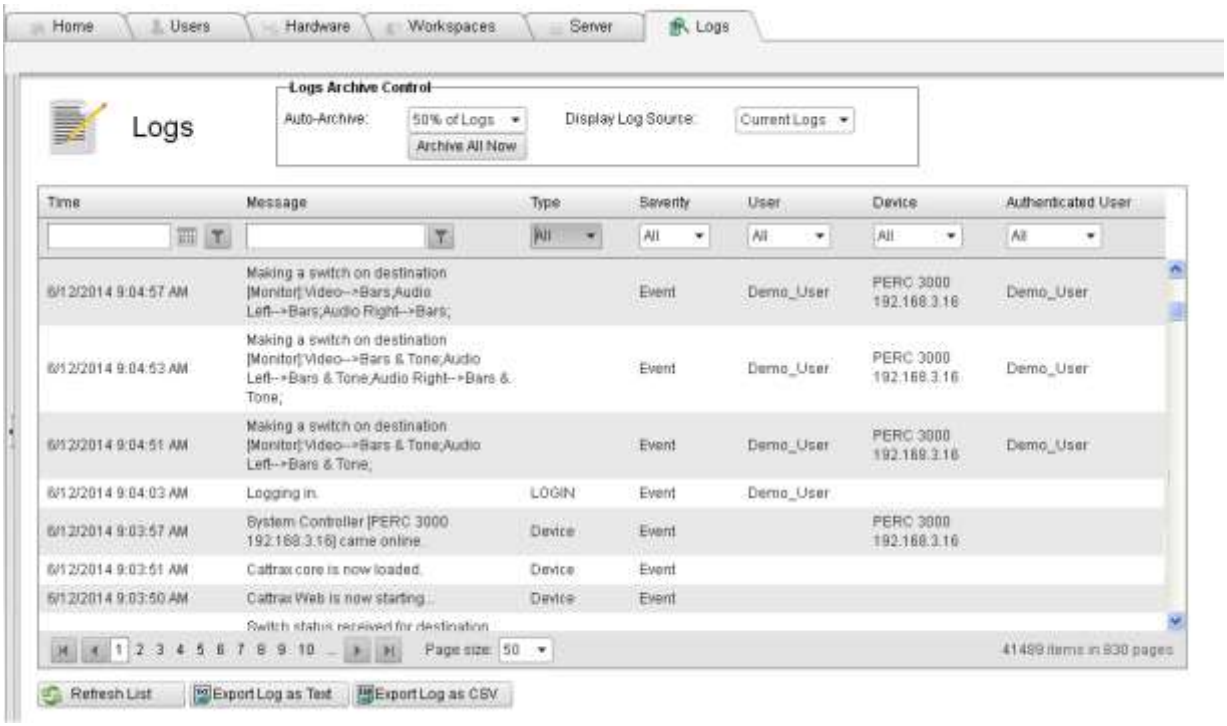


Figure 5-17 Logs Page

- **Log Table**

  The log table records various events and conditions during operation of the Cattrax Web application. The following parameters are recorded as applicable for each log entry:

  - **Time** – Records the time of day the event or condition occurred.
  - **Message** – Displays a brief description of the condition or event.
  - **Type** – Identifies the type of log entry message as follows:
    - Login and Logout – Indicates when a user logs in or out of Cattrax-Web.
    - Admin - Indicates when a user related change is made. For example a new user added.
    - Object – Indicates when a configuration related change is made.
  - **Severity** – Identifies the severity of the log entry message as one of the following three levels:
    - Event – Indicates something is changed or detected from the device and is not a problem.
    - Warning – Indicates some issue the user needs to know but not considered to be an Error. For example an attempt to make a switch on a destination that is locked.
    - Error – Indicates an event which needs user's attention. For example, change in device online status.

- **User** – If the log entry pertains to a particular user, the username configured through Cattrax Web for that user is displayed in this column.
- **Device** – Identifies the hardware system controller associated with the event or condition.
- **Authenticated User** – If the log entry pertains to a particular user, the Windows username for that user is displayed in this column, if the Windows authentication function is activated for the web server.

- **Log Table Pagination**

  Navigation controls to access log pages are located at the lower left of the log table. You may choose a specific page by clicking the desired page number, you may move forward or backward through the pages by clicking the left or right facing single arrow button, or you may jump immediately to the first or last page by clicking the left or right facing button with an arrow followed by a vertical line.

  The page size drop-down allows you to select the number of log entries that appear on each page, and the counter in the lower right of the table keeps a running count of currently active log entry items and log pages.

- **Logs Archive Control**

  Cattrax Web holds up to 10,000 log entries, after which older entries will begin being removed to make space for newer entries. If you wish to maintain a permanent record of system logs, you may choose to manually archive log data, or allow Cattrax Web to automatically archive logs at specified intervals.

  You may manually create a log archive file from the current log entries at any time by clicking the *Archive All Now* button. You will be prompted to verify the requested action. Once the log entries have been archived, all currently displayed entries will be removed from the display and from system memory.

  Auto-Archive is always active; however, Cattrax Web gives you the option to choose the interval at which logs are archived based on the percentage of memory capacity currently used for retention of logs. The drop-down list gives you the option of 25, 50 of 75% of log storage capacity. For example, if you have selected 50% as the auto-archive interval, when the currently displayed log entries reaches 50% of maximum storage capacity, the entries are automatically archived and removed from system memory.

  The Display Log Source drop-down opens to a list of log archive files. If you wish to open a log archive, select the archive file to view from the drop-down. If you choose Current Logs from the list, the log table displays the currently active log entries.

- **Refresh List –** Refreshes the log table entries
- **Export Log as Text –** Cattrax Web will create and write a text file containing current log entries. You will be prompted to enter a file name and browse to a location where you want the file written.
- **Export Log as CSV –** Cattrax Web will create and write a comma separated variable (CSV) file containing current log entries. You will be prompted to enter a file name and browse to a location where you want the file written.

5.18 SWITCHING PAGE

The Switching page, Figure 5-18, is where authorized users of any privilege level can check router status or make switches, i.e. change source to destination connectivity in the router. It is also the default home page for staff level users. Through the Switching page, individual users or members of a user group are allowed access to the devices, destinations, sources, levels and salvos for which they are authorized by the Cattrax Web workspace configuration.

There are five basic functional areas to the Switching page, as shown by Figure 5-18:

1. **Menu Bar** — The four menu bar buttons open pull-down menus which allow you to select various control options for the switching page. Refer to paragraph 5.18.
2. **Workspace Header** — Allows selection and status monitoring of the workspace currently in use. Refer to paragraph 5.19.
3. **Switching Area-** — This area contains the actual router status and control functions of Cattrax Web. Refer to paragraphs 5.20.1 thru 5.20.4.
4. **Salvo Window -** — This fly-out window allows the user to view a list of system and local salvos available through the workspace. Salvos may be fired from this window, and local salvos may be selected for editing. This window may be pinned to remain open, if desired. Refer to paragraph 5.21.
5. **Log Display -** — Opens a fly-out display area for real-time switching and system operation logs. This window may be pinned to remain open, if desired. Refer to paragraph 5.23.

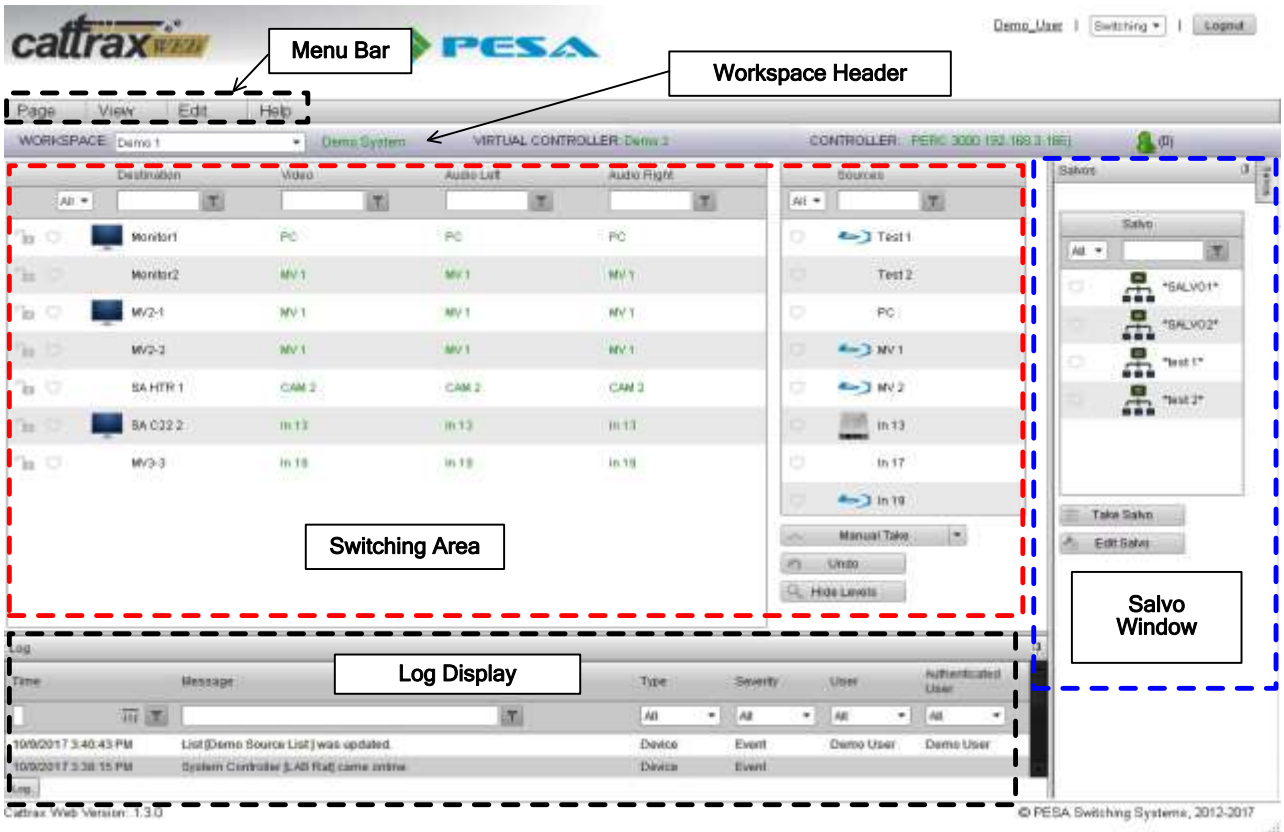
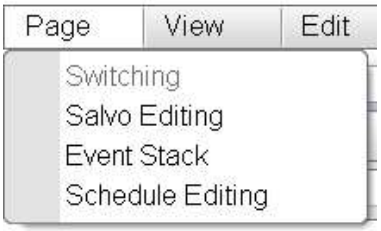


Figure 5-18 Example Switching Page

5.19 MENU BAR

Page Menu – The Page menu opens to a listing of control pages, as shown here, which may be accessed from the Switching page.



Switching is the default selection and selects the switching home page for display.

Salvo Editing opens the *create and edit* page for local salvos. Refer to paragraph 5.22.

Event Stack (only available when the optional Event Scheduling feature is licensed and active) opens the display and status page for switching events scheduled through the Schedule Editing page. Refer to Chapter 6 for information on the optional Event Scheduling feature of Cattrax Web.

Schedule Editing (only available when the optional Event Scheduling feature is licensed and active) opens the control page for configuration and editing of automated scheduled switching events. Refer to Chapter 6 for information on the optional Event Scheduling feature of Cattrax Web.

View Menu – The View menu opens to a listing of toggle functions that allow you to quickly open/close the flyout display windows or hide/unhide the switching level columns.

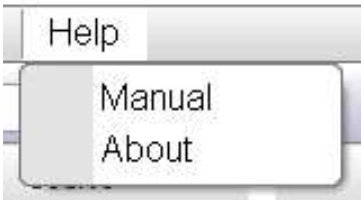
Toggle Log opens and closes the *Log Display* window. Refer to paragraph 5.23.

Toggle Salvos opens and closes the *Salvo Window*. Refer to paragraph 5.22.

Toggle Levels unhides and hides the level display columns in the *Destination* display window. Refer to paragraph 5.20.

Edit Menu – The Edit menu contains controls that allow you to simultaneously lock or unlock all destinations in the Destination table. Refer to paragraph 5.20.2

Help Menu – The Help menu contains information about Cattrax Web.



Manual opens an on-screen copy of the Cattrax Web User Guide.

About displays revision information about the currently running version of the Catrax Web application.

5.20 WORKSPACE HEADER

The workspace drop-down list, subsystem, virtual controller, hardware system controller associated with the selected Switching page and the number of users logged into the workspace are shown in the workspace header bar above the matrix table display area.

Opening the drop-down list provides a listing of all workspaces to which the logged-in user is granted access.

Open the list and select the workspace containing the router resources you want to monitor or switch. Select "All Workspaces" if you wish to open all authorized workspaces.

The selection is maintained while the user is logged in so that if the user navigates to a different page, for example the Salvo Configuration page, the selected workspace is redisplayed when the user returns to the Switching page.

5.21 SWITCHING AREA

There are two tables in the display area. Router destinations authorized for user access are shown on the left side of the display area. The current router matrix status can be viewed from this table with or without all available switching levels shown. With all switching levels displayed, the source switched to each listed destination for each level is shown in the columns to the right of the *Destination* column.

When the levels are hidden (hidden mode) a *Source* column is shown that reflects sources switched to each listed destination through the Status Level of the subsystem, as defined through the Subsystems configuration page. Refer to paragraph 5.10.4.

Also in hidden mode, a source listing for any destination displayed in a color different from the destination entry indicates that the source for at least one of the switching levels for that destination is different, i.e. the destination is in a breakaway condition.

You can toggle the level display mode by clicking the *Show Levels/Hide Levels* button to the lower right of the switching display area.

The table to the right of the matrix table lists all available router source signals that may be switched to the destinations authorized for the workspace.

If desired, Cattrax Web allows you to place a graphic icon beside destination or source entries for quick identification, as shown in Figure 5-18. The icon display function may be activated or deactivated through a menu selection on the Server Configuration page. Refer to paragraph 5.13.2.

Every table column contains a filter function that allows you perform a data search for a specific character or character string you wish to locate in the column. Enter the search parameter in the data entry box at the top of the column you wish to search. Clicking the filter icon next to the data entry box opens a drop-down menu listing of criteria you may use to refine your search.

You may sort the content of columns that offer sorting capability by clicking the column name header. The column header *Destination* for example, sorts the table in alphabetical order based on the entries in the Destination column. Clicking the header again, reverses the order of sorting, and a third click returns the column to the default display order by the configuration sequence number of the system resource.

5.21.1 PERFORMING A SWITCH ON THE ROUTER

Authorized users can take switches on the router in either All Levels or Breakaway switching modes through the matrix table.

All Levels Switch

When an All Levels switch is performed, all destination switching levels for which the selected source group contains a valid signal input will be switched to the newly selected source signal(s). To perform an All Levels switch, click the destination name you wish to switch in the Destination column of the matrix table. The destination name will not be highlighted, however all switching level entries on the row will be selected and highlighted. Select the desired switching mode (see Switching Mode, below) and initiate the switch in accordance with the procedure presented.

Breakaway Switch

When a Breakaway switch is performed, only the selected destination switching levels will be switched to the newly selected source signal(s). To perform a Breakaway switch, expand the matrix table to show all switching levels by clicking the *Show Levels* button. Locate the destination name you wish to switch in the Destination column of the matrix table. Click the row entry in each switching level column that you wish to switch. The selected column cells will be highlighted. Select the desired switching mode (see Switching Mode, below) and initiate the switch in accordance with the procedure presented.

Switching Mode

Depending on the switching mode selected, you may have a switch occur immediately upon source selection or allow you to select the source and then manually initiate the switch.

The switching mode drop-down button allows you to select any of three available switching modes:

- **Manual Take** – (default) – User selects the desired destination and source for the switch, followed by clicking *Manual Take*. In this mode it is also possible to double-click on the source entry to make the switch.
- **Hot-Take Source** – In this mode the user can select an All Levels or Breakaway switch for a destination and then click on a source to immediately perform a switch on the selected switching levels.
- **Hot-Take Destination** – In this mode the user can select a source and then click on a destination or a level to immediately initiate a switch.

Select the desired switching mode and initiate a switch on the router as follows:

- Locate the entry in the *Destination* column that you wish to switch and select the switching levels on which you wish the switch to occur using either an All Levels or Breakaway switch.
- Click the source name you wish to switch to the destination in the *Sources* table.

5.21.2 DESTINATION LOCK MODES

Applying protection to a destination prevents another user or an accidental key press from switching the current source selection. Lock Modes may be selected by clicking the *padlock* icon in the first column of the matrix table on the row of the destination you wish to protect. Each click on the icon toggles between three available lock modes:

- **Unlocked** – (Open Padlock icon) – Destination is unlocked and can be switched by any authorized user or hardware panel.
- **Protect** – (Shield Icon) – Clicking the padlock icon on a destination row once places the destination in “Protect” mode, whereby the protected destination can still be switched by another instance of Cattrax Web using the same workspace as the originating user. Hardware panels can not make a switch on the destination with the protect mode in place. However, any hardware panel with lock/protect capability can cancel the protect function and make a switch on the destination.

- **Lock** – (Latched Padlock Icon) – Clicking the shield icon places the destination in "Lock" mode. In Lock mode the selected destination is "Locked" for all users and can not be switched to a different source by another instance of Cattrax Web or by a hardware panel without first unlocking the selected destination. Any Cattrax Web user or any hardware panel with lock/protect capability can cancel the lock function and make a switch on the destination.

NOTE	In all cases, another instance of Cattrax Web or a hardware panel with lock/protect capability can change the lock mode status. Cattrax Web logs any changes as to when they were made and by whom.

Destination locks may also be applied to (*Lock All*) or removed from (*Unlock All*) all destinations simultaneously using pull-down menu selections available from the Edit menu on the menu bar. Refer to paragraph 5.18.

5.21.3 FAVORITE DESTINATIONS

To allow quick access to often used destinations, Cattrax Web allows you to designate any destinations you wish from the matrix table as favorites. Once you have designated one or more destinations as a favorite, you may apply the favorites filter by opening the drop-down box at the top of the column. Select the *Fav* entry to display only favorite destinations. Selecting *All* from the drop-down box returns all destaintions to the matrix table display.

To designate a destination as a favorite, click the heart-shaped icon in the second column of the matrix table on the row of the destination you wish to make a favorite. When selected, the heart is highlighted. To cancel the favorite designation, click the icon again to de-select the heart.

5.21.4 UNDO FUNCTION

Clicking the *Undo* button toggles between the current and the last switch status.

5.22 SALVOS WINDOW

Open the **Salvos** window panel by clicking the *Salvos* tab on the right edge of the Switching page display. An example panel is shown at right. In normal operation, this panel is a fly-out window and will return to hidden when the cursor is moved out of the window. If desired, you may choose to keep the panel open by clicking the push-pin symbol in the header bar. This panel contains a list of system and local salvos.

System salvos are defined by the system configuration and shown in the list with an asterisk '*' at the start and end of the salvo name. Example – *Test1*, as shown. A salvo can be fired at any time by selecting the salvo and clicking the *Take Salvo* button.

Salvos may be viewed and local salvos may be modified by selecting the salvo and clicking the *Edit Salvo* button. Refer to paragraph 5.17. System salvos can not be modified through Cattrax Web.

5.23 SALVO CONFIGURATION (CREATE AND EDIT SALVO PAGE)

The Salvo Configuration page, Figure 5-19, displays system salvos, and allows a user to create and edit local salvos.

There are two ways to access the Salvo Configuration page:

- From the fly-out Salvos window on the Switching page, select the salvo entry from the table list that you wish to edit. Click the *Edit Salvo* button beneath the table to open the Salvo Configuration page to the selected salvo entry.
- Open the Page menu on the menu bar and select *Salvo Editing* from the options list.

The table on the left side of the page displays a listing of all system salvos and local salvos. System salvos are those defined by the system controller configuration file, and cannot be edited or deleted through Cattrax Web. System salvos are shown in the list with an asterisk '*' at the start and end of the salvo name. Example – *BarsTone*, as shown by Figure 5-19.

To the right of the salvo list table are three columns that list, from left to right, available destinations authorized for the workspace, the salvo display area that identifies destinations and sources currently configured for the salvo selected in the name list, and the third column lists the sources that are authorized for access by the workspace.

Local salvos are created through the Salvo Edit page and are available only to users of the workspace shown at the top of the page. When either a system salvo or local salvo is selected from the list, the destinations and sources switched by the salvo are displayed in the salvo display area.

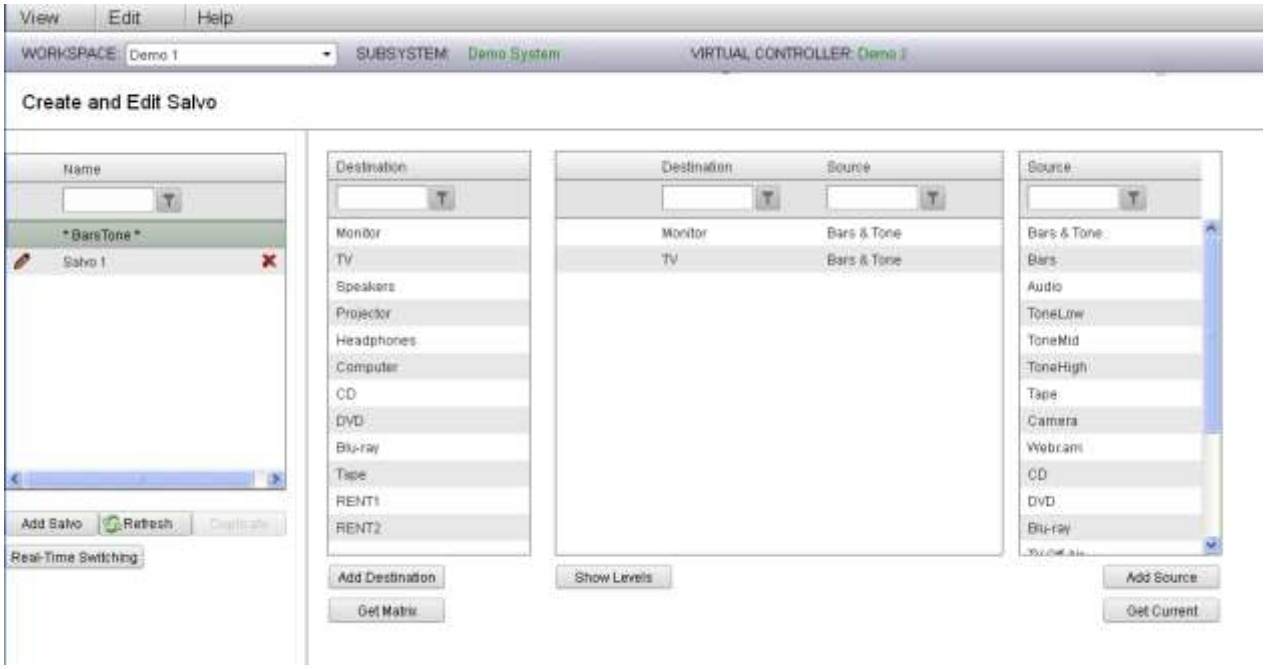
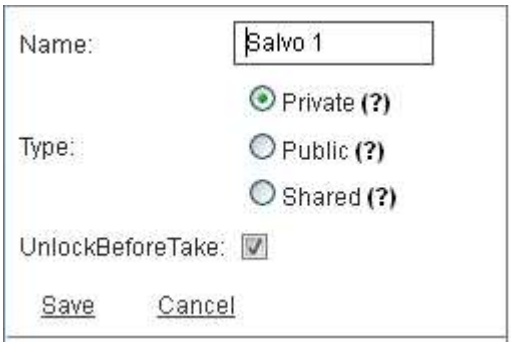


Figure 5-19 Salvo Edit Page

A local salvo must first be created in the salvo column on the left side of the page, and then configured by selecting entries from the destination and source columns with the matrix table in the middle. The *Add Destination* and *Add Source* buttons may be used to configure the local salvo.

You may add, delete or edit a local salvo as follows:

- Click the *Add Salvo* button to open the pop-up dialog box, as shown below.



- Enter a name for the new local salvo in the box beside the prompt.
- Click the radio button to assign the local salvo type from the following options:
  - **Private** – Only the current user can take or edit this local salvo.
  - **Public** – All users in this workspace can take this local salvo, but only the current user can edit it.
  - **Shared** – All users in this workspace can take or edit this local salvo.
- If any of the destinations switched by the local salvo are locked at the time the salvo is fired, placing a check in the *Unlock Before Take* box allows all destinations in the salvo to be unlocked and the switch to occur. Once the switch initiated by the salvo has occurred, the destinations will remain unlocked.
- Click *Save* to create the new local salvo.
- Ensure that the new salvo name is selected and highlighted in the list.
- Select the destinations you wish to include in the newly created salvo from the Destination list and click the *Add Destination* button beneath the destination list table.
- Click the *Show Levels* button if you wish to expand the salvo display area to include all switching level columns. Click the destination name in the salvo display area to select all switching levels for an All Levels switch. Click the cells in the switching level columns of the levels you wish to include if configuring a Breakaway switch salvo. The switching level cell must be selected and highlighted before a source can be assigned to it.
- Locate the source you wish to switch to the salvo destination in the Sources list table and click the *Add Source* button beneath the table to add the source to the selected switching level cells.
- The local salvo entries are automatically saved as they are entered.
- If you select any local salvo name from the list and click the *Duplicate* button, a new local salvo identical to the selected salvo is created. You may use the edit command to rename the new salvo and make any changes to the destination and source entries from the salvo display table. This feature is often helpful if you need to create a new local salvo with only slight differences to an existing one.

- To delete a local salvo, click the *red "x"* at the right edge of the name entry you wish to delete. You will be asked to confirm the action before the component is removed.
- You may edit the name, type or unlock permission of a local salvo by clicking the *Pencil Icon* to the left of the name you wish to edit.
- Make any desired changes to the name or other data in the dialog box and click Sa*ve* to retain the change.
- Click C*ancel* to exit the dialog box with no change.

Get Matrix and *Get Current* buttons are provided to allow the user to display the current status of the routing switcher matrix as the starting configuration for creating or editing a local salvo. Get Matrix retrieves status of the entire matrix, while Get Current retrieves matrix status of only the selected destination or switching level.

Note that local salvos are workspace specific, therefore the workspace selected from the workspace drop-down list displays only local salvos for that particular workspace. System salvos are displayed in the name list regardless of the workspace selected.

Click the *Real-Time Switching* button to return to the Switching page.

5.24 LOG DISPLAY

Open the **Logs** panel by clicking the *Logs* tab at the lower left-hand edge of the Switching page display. In normal operation, this panel is a fly-out window and will return to hidden when the cursor is moved out of the window. If desired, you may choose to keep the panel open by clicking the push-pin symbol in the header bar.

Log panel displays a log of all switches made for the currently active workspace by all users of that workspace. It provides the user an instant notification of changes in the active workspace, including changes in device online/offline status, changes in lock status etc. The Logs panel display defaults to auto-hide mode.

Chapter 6 Event Scheduling Option

6.1 INTRODUCTION

Event Scheduling is an optionally available feature for Cattrax Web that adds automated source to destination switching control to a PESA routing system installation by allowing you to create schedule items (switching events) to automatically occur on a date and clock time basis.

Use event scheduling to switch program sources such as promotional presentations, movies or other program material to router output destinations for delivery to distribution channels, recording devices, etc.

Once schedule items are configured, Cattrax Web does not have to be open in a browser for the scheduled switching functions to occur. Each scheduled switching event may be performed as a non-breakaway switch or salvo and can be scheduled to occur once, repeat daily or repeat on specified days only.

The event log keeps a record of all scheduled switching events as they are processed by Cattrax Web.

6.2 OVERVIEW

Every automated switch command sent to the router by the Cattrax Web event scheduling feature is called an *event*, and every event that you want to occur must be configured by creating a *schedule item* for that event. When a schedule item is created, the following information about the event (switch occurrence) is defined:

A name and description is given to the event,

the date and time you want the event to occur and, if the event repeats, the time period (range of dates) over which you want the multiple occurrences of the event to take place,

the type of switch and the router resource parameters you want to switch when the event is "fired".

Once a schedule item is created, the event it defines is added to the master schedule of pending events, called the *Event Stack*, refer to paragraph 6.3. If the schedule item is repeating, all events it defines will be added to the event stack page.

Schedule items are also listed on the *Schedule Editing* Page, where individual schedule items may be reviewed, edited or deleted as required. New schedule items are created through the schedule editing page as well. Refer to paragraph 6.4.

User interface for event scheduling is through dedicated operator pages of Cattrax Web, accessed from the Switching page for the active workspace the user is logged in to. Schedule items created through a particular workspace are specific to that workspace, meaning that router access is controlled by limiting the system resources available for creating switching events (schedule items) to the resources for which the workspace is granted control.

Before we look at the event scheduling interface pages or how to create a schedule item, let's look at an example of a typical event.

Suppose we want a switch to occur on the router which would feed the output signal from a specific video player over a community distribution TV channel at 4 PM on a specific date. Let's assume that the video signal enters the router as source *Player 2* and the distribution equipment for the TV channel derives its input source from router output *TX 2*. We could create a schedule item for the event and name it *Evening Announcements*, for example. We would enter the Start Date and Time (4 PM on the desired date) for the

event (router switch) to occur, and then select Player 2 as the source for destination TX 2 as the router resource parameters for the event. Once the schedule item is created, Cattrax Web adds the event it defines to the event stack of pending scheduled events.

If we want to switch the signal from this video player to this distribution channel every evening at 4 PM instead of just once, we can configure the schedule item to repeat. Cattrax Web allows you to define a date and time you want the event to first occur (Start Date/Time) and a date and time you want to be the last occurrence of the event (End Date/Time).

User interface pages for event scheduling are discussed in the following paragraphs.

6.3 EVENT STACK PAGE

Open the Event Stack page by clicking *Event Stack* in the *Page* menu drop-down list, as shown at right.

The event stack page displays a real-time listing of scheduled events in chronological sequence. If a schedule item defines a repeating event, there may be multiple entries of the event shown in the event stack.

Cattrax Web also allows you to issue a master pause command from the event stack page that halts all event processing until the pause command is manually removed. Refer to paragraph 6.3.2.

6.3.1 EVENT STACK DISPLAY MATRIX

Each event in the stack is shown on an individual row, with the last five processed events and the next event in queue to be processed displayed on color highlighted rows at the top of the page.

A “processed” event is a schedule item whose defined start date and time has passed, and for which a switch command should have been sent by Cattrax Web to the router, unless the event was on “hold” at the time it was processed.

If an event is on “hold” or for some other reason is unable to be “fired" at its scheduled time, Cattrax Web will continue to try to process that event for one minute. If the repeated attempts are not successful, the event is marked as “failed”.

The five most recent events are shown highlighted in green if the event was successfully processed and highlighted in red if event processing failed and a switch command was not sent to the router.

The next event to be processed is highlighted in yellow. The Status column indicates the action taken by Cattrax Web at the time the event was processed.

An example Event Stack page is shown by Figure 6-1. Each column of the display matrix is introduced below:

- **Order** – The left-most column of the page displays the sequence number for each event. Sequence numbers for processed events are shown with a plus (+) sign preceding the number, with plus one (+1) being the most recently processed event. Pending, or unprocessed, events are shown with a minus (-) sign preceding the number. Sequence numbers for pending events indicate the “firing” order for scheduled events.
- **CountDown** – The CountDown column displays in the format of <days, hours, minutes, seconds> the amount of time that has lapsed since a processed event was processed (count-up time), or the amount of time until a pending event is due to be processed (countdown time). Count-up time for a processed event is shown with a plus sign (+) preceding the time display; count-down time for a pending event is shown with a minus sign (-) preceding the time display.

Figure 6-1 Example Event Stack Page

- **Date/Time** – The Date/Time column displays the scheduled date and time at which the listed events will occur.
- **Status** – Symbols used in the Status column indicate real-time status of each event shown on the page from the following options:

  Green Check Mark – Indicates the processed event was "fired" (switch command was sent by Cattrax Web to the router) at the date and time scheduled.

  Orange "X" – Indicates the processed event DID NOT fire because the event was on "hold" at the time the event was scheduled to occur.

  Red "X" – Indicates the event was not on "hold" at the time it was scheduled to occur, but for some unknown reason the switch command did not get sent to the router. This could occur if, for example, the Cattrax Web server was not running at the time the event was scheduled.

  A common, universal "pause" symbol (two parallel, vertical bars) is used to show the "hold" status of each pending scheduled event shown on the page.

  Hold Symbol - bars shown in green – Indicates the event is not currently on hold.

  Hold Symbol - bars shown in red – Indicates the event is currently on hold, and will not fire at its scheduled time.

  Hold status may be applied to an individual event shown on the event stack page by clicking the hold symbol on the row of that event entry. Only the selected event will be held. All other event stack entries for the schedule item will remain active.

  You may remove the hold status from any event by clicking the red hold symbol for the event stack entry. The hold symbol will return to green and the event will fire at its scheduled time.

- **Name** – Displays the name assigned to the event when the schedule item was created.
- **Source/Dest/Salvo** – These columns identify the system resources for the switch command that will be issued by Cattrax Web to the router when the event is processed.

  If the event schedule is a defined source/destination switch, the source name and destination name along with their identification icons, if used, will be shown in their respective columns.

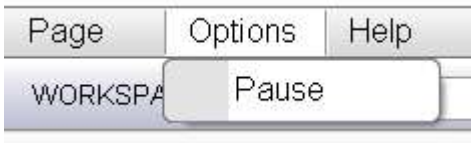
  If the event defines a salvo, the salvo name and its identification icon, if used, will be shown in the Salvo column.
- **Repeat –** If the schedule item defines a repetition schedule for the event, the repeat frequency (Daily, for example) will be shown in this column.

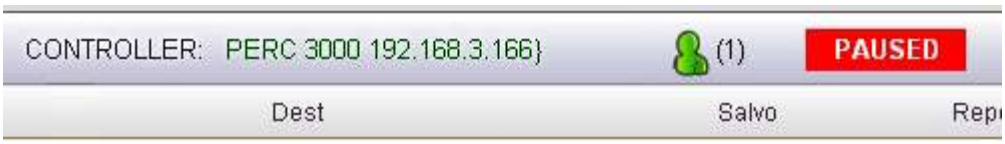
6.3.2 MASTER EVENT SCHEDULING PAUSE

You may manually issue a master pause command for the event scheduling function from the event stack page. When event scheduling is paused, no events will be processed.

Manually pause event scheduling as follows:

1. Click the *Options* button on the menu bar to open the list box as shown at right.
2. Click the *Pause* command from the list.
3. When the system is in pause mode, a red warning box is displayed at the top of the page as shown below.





4. To remove the pause command, open the *Options* box and click the *Pause* command entry. Repeatedly clicking the *Pause* command entry toggles the system pause function.

6.4 SCHEDULE EDITING PAGE

Open the Schedule Editing page by clicking *Schedule Editing* in the *Page* menu drop-down list, as shown at right. An example schedule editing page is shown by Figure 6-2.

The schedule editing page allows an operator to review, edit, pause or delete event schedule items. Event schedule items are shown on individual rows. You may sort the page contents by entering search text in the box beneath the column header name of the column you wish to search.

The configuration page for creating new schedule items is also accessed from this page.

Regardless of whether an event is a one-time occurrence or repeated, when a schedule item is created, an entry for the event is displayed on the schedule editing page. All schedule items remain listed on the schedule editing page until manually deleted by an operator, even if an item has passed its end date and time.

Outdated schedule items will no longer be placed in the pending event queue (event stack), but will remain on the schedule editing page so that you may easily restore the event to active status, if needed, without having to recreate the schedule item. You may edit the outdated event to change the end date or time to some time in the future and reinstate the event as a pending item in the event stack.

To edit the schedule item for any of the listed events, locate the schedule item you wish to edit and click the yellow pencil icon at the right edge of the row to open the schedule item configuration box for the event. Make any changes needed to the schedule item entries and click the *Insert* button at the bottom of the box. Refer to paragraph 6.5 for more information on the schedule item configuration box.

Each column of the schedule editing page is introduced below:

Figure 6-2 Example Schedule Editing Page

- **Name** – Displays the Name assigned to the event schedule when the event was created. Entering text in the filter box just below the Name header will alphanumerically sort the contents of the column.
- **Description** – Displays the Description text entered for the event schedule when the event was created.
- **Source/Dest/Salvo** – These columns identify the defined system resources for the switch command that will be issued by Cattrax Web to the router when the event is processed.

  If the event schedule is a defined source/destination switch, the source name and destination name along with their identification icons, if used, will be shown in their respective columns.

  If the event defines a salvo, the salvo name and its identification icon, if used, will be shown in the Salvo column.

  You may sort the contents of any of the columns by entering alphanumeric search text in the filter box just below the column header of the column you wish to sort.

- **Repeat –** If the schedule item applies a repetition schedule to the event, the repetition frequency (Daily, for example) will be shown in this column. The pull-down arrow in the box just beneath the Repeat column header opens a list of search terms by which you may sort the column contents.
- **Start –** Displays the date and time for the first occurrence of the scheduled event.

  You may sort the display matrix by the contents of this column by selecting a date and time, or a range of dates/times, by which you wish to search. To enter a range, enter the beginning search date and time in the filter box on the left, and the ending search date and time in the filter box on the right. Click the calendar icon to the right of the filter box to select a date, or click the clock icon to select a time. The selected search parameter will be inserted in the filter box.
- **End –** Displays the date and time for the last occurrence of a repeating scheduled event.

  You may sort the display matrix by the contents of this column by selecting a date and time, or a range of dates/times, by which you wish to search. To enter a range, enter the beginning search date and time in the filter box on the left, and the ending search date and time in the filter box on the right. Click the calendar icon to the right of the filter box to select a date, or click the clock icon to select a time. The selected search parameter will be inserted in the filter box.
- **Pencil Symbol** – Clicking the pencil symbol on any row opens the event schedule editing box for the selected event. You may make any changes desired to the event schedule through the editing box.
- **Red X Symbol** – Clicking the red X symbol on any row deletes the event schedule. You will be prompted to verify the action before the event schedule is deleted.
- **Create Schedule Item** – Clicking the *Create Schedule Item* button at the bottom of the page opens the event schedule creation box where you can configure new event schedule items. Refer to paragraph 6.5.

6.5 CREATING SCHEDULE ITEMS

In order to use Cattrax Web event scheduling, a schedule item must be created for each event which defines:

- The source to destination switch(es) to occur when the event is "fired",
- the date/time at which the event is to occur,
- whether or not the event is to repeat and the range of dates over which you wish a repeating event to occur.

The event schedule may specify an individual destination and source or a named salvo may be specified for the switching function.

Remember that once a router switch is initiated by Cattrax Web event scheduling, the router source(s) and destination(s) switched by the event remain connected until another switch command from any router control device changes the matrix status. The End Date/Time specified for a repeating schedule item defines the period of time over which the events added by the schedule item will appear as pending events in the event stack. This parameter does not cause any change to occur on the router switching matrix.

For easy entry when creating schedule items for common or often used events, PESA recommends that you create a local salvo for such events. Assign the salvo a name that easily identifies the event.

Schedule items can only be created using system resources available to the workspace in which the schedule editing page is open.

To create a Schedule Item, click the *Create Schedule Item* button at the bottom of the schedule editing page to open a blank event schedule creation box.

An example Schedule Item Creation Box is shown by Figure 6-3. Each field of the box is introduced in the following paragraphs.

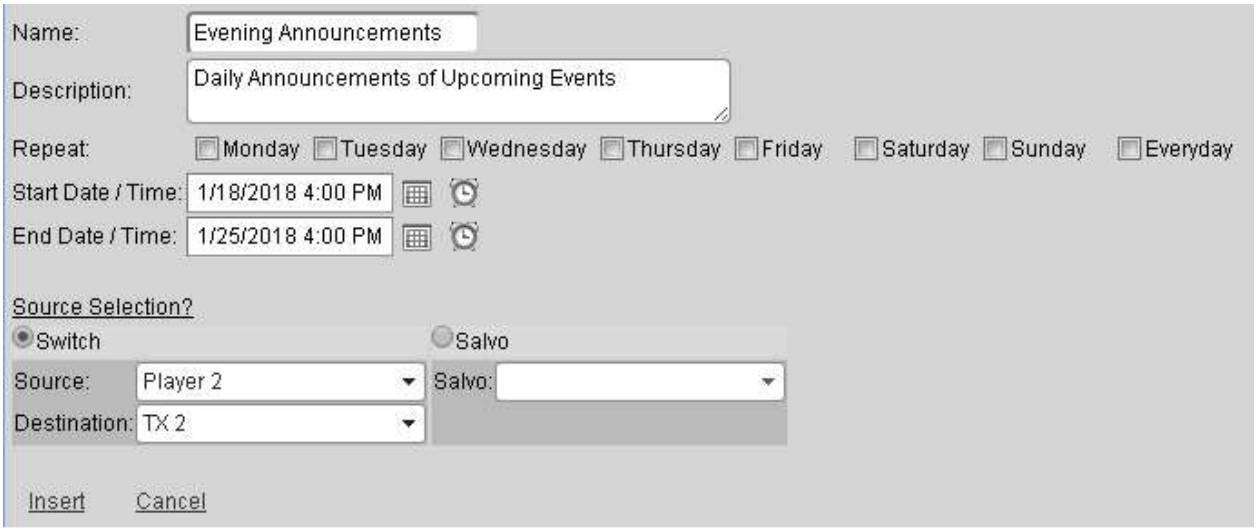


Figure 6-3 Example Schedule Item Creation Box

- **Name** – Enter a Name you wish to assign to the event schedule you are creating.
- **Description** – Enter a text Description you wish to associate to the event schedule you are creating. PESA recommends that you use a name that is descriptive of the function or content of the event.
- **Repeat** – Allows you to apply repeat options to the event schedule. From this listing, you may select specific days of the week on which you would like the event to repeat. Check the box beside the day or days you wish to select, or you may choose Everyday to place a check in all daily selection boxes.
- **Start Date/Time –** Allows you to enter the desired date and time for the first occurrence of the scheduled event.
- **End Date/Time –** Allows you to enter the desired date and time for the last occurrence of the a repeated schedule event.
- **Source Selection** – There are two radio buttons beneath the Source Selection header that allow you to select the type of switch defined by the event from the following options:

  Switch – Selecting the *Switch* button defines the event switch as a non-breakaway source to destination switch. Use the pull-down lists beneath the radio button to select the source and destination for the event switch.

  Salvo - Selecting the *Salvo* button defines the event switch as a salvo switch. Use the pull-down list beneath the radio button to select the pre-configured salvo for the event switch.

  Sources, destinations and salvos shown in the pull-down lists are the system resources available to the workspace currently selected on the switching page.
- **Insert –** Activates the schedule item. Events defined by the schedule item will be added to the Event Stack page and the schedule item will be added to the Schedule Editing page.
- **Cancel** – Cancels the operation and closes the schedule item creation box.

Chapter 7 In the Event of Difficulty

7.1 PESA Customer Service

If you have questions about, or are experiencing any difficulty with, your Cattrax Web system control application, contact PESA's Customer Service Department. Technicians are available to assist you 24 hours a day, seven days a week.


PESA