

StorLogix
StorLogix
StorLogixTM
StorLogix
StorLogix
StorLogix
StorLogix
StorLogix
StorLogix
StorLogix
StorLogix
StorLogix
StorLogix
StorLogix
StorLogix

***installation and
setup manual***

StorLOGIX

Installation and Setup Manual

Copyright

© 2000-2005 Preferred Technology, Inc., dba PTI Integrated Systems. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, or translated into any language in any form, by any means, without written permission of Preferred Technology, Inc., dba PTI Integrated Systems.

Trademarks

Falcon XT™, StorLogix™, “Security Without Limits”™, LogixServer™, LogixScript™, VideoViewer™, EventViewer™, PTI Site Graphics™, “Easy to Implement, Simple to Use”™, are trademarks of Preferred Technology, Inc., dba PTI Integrated Systems. All rights reserved.

Microsoft Windows 2000®, Microsoft Windows XP®, Adobe Reader®, Symantec pcAnywhere®, Pentium®, McAfee Virus Scan®, Norton Antivirus® and all other trademarks referenced are the property of their respective owners.

Contents

Welcome	v		
Using This Manual	v		
Product Overview	vi		
Specifications	viii		
1: Pre-Installation	1	4: Device Setup	69
Installation Recommendation	2	Enroll AI Devices	70
Training Recommendation	2	Setup Relays	72
System Requirements for StorLogix	3	Setup Relays - Advanced	74
Computer Requirements	4	Virtual Relays	75
Other Requirements for StorLogix	6	Setup Inputs	76
Pre-Installation Worksheet	7	Setup Inputs - Advanced	78
Chapter Terms	22	Chapter Terms	80
2: Loading the Software	27	5: Site Setup	83
Beginning the Install	28	Setup Alarm Zones	84
Loading the MSDE	29	Setup Alarm Zones - Advanced	86
Loading Adobe Reader	30	Setup Lighting Areas	87
Loading Easy Link	33	Setup Lighting Areas - Advanced	89
Loading StorLogix	35	Setup Buildings	90
Loading LogixServer	38	Setup Elevators	92
Desktop Icons	41	Chapter Terms	95
Demonstration Mode	42		
Registering the Software	43	6: Access & Authorization Setup	97
Software Activation	44	Setup Access Areas	98
Chapter Terms	45	Setup Access Areas - Advanced	100
		Setup Access Levels	102
3: General Setup	47	Setup Access Levels	102
Initial Database Setup	48	Setup Operators	104
Initial StorLogix Setup	49	Chapter Terms	106
Setup LogixServer	51		
Logging In to StorLogix	53	7: Unit Setup	109
Navigation in StorLogix	54	Setup Units	110
Setup Preferences	55	Setup Inputs to Units - Basic	114
Setup Screen	56	Setup Inputs to Units - Advanced	115
Setup Company Info	57	Importing Units and Inputs to Units	116
Setup Security Levels	59	Exporting Units and Inputs to Units	118
Setup Time Schedules	63	Chapter Terms	120
Chapter Terms	67		

8: Device Configuration Setup	123	11: Troubleshooting	191
Setup AI Device Properties	124	Troubleshooting Concepts	192
Setup AI Device Properties - Advanced	126	Troubleshooting Gates	194
Setup Falcon XT	129	Troubleshooting Access Issues	196
Setup Falcon XT - Advanced	131	Troubleshooting Door Alarms & Inputs	198
Chapter Terms	134	Troubleshooting Computer Issues	201
 		Troubleshooting Communications	202
9: Optional Setup	139	Troubleshooting Networking Issues	203
Setup DVR	140	 	
Setup Holidays	143	12: Appendix	205
Setup Events to View	145	Falcon 2000 to Falcon XT Cross Ref	206
Chapter Terms	147	Notices, Warnings, and Declarations	214
 		End User License Agreement (EULA)	217
10: Other Setup	149	Standard 2-Year Equipment Warranty	224
Setup Cards	150	Contact PTI	225
Setup Custom Messages	153	Glossary	226
Custom Messages Assigned to Users	158	Index	240
Alerts	160		
Inputs to Relays	164		
Networking StorLogix	166		
Interface to TaskMaster	176		
Interface to other Accounting Software	177		
LogixScript	180		

Welcome

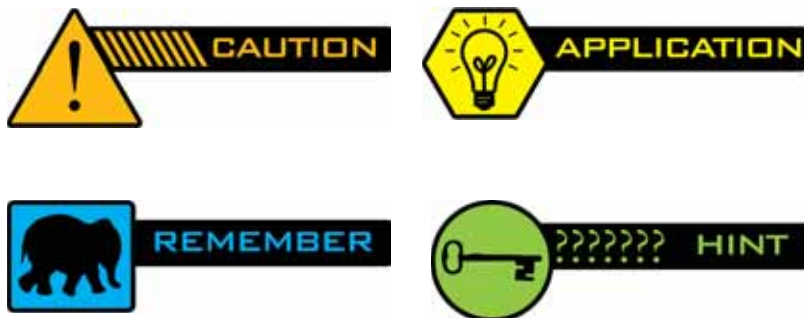
Thank you for purchasing the StorLogix Access Control Software. For your utmost satisfaction with this product, we recommend that you take the time to review this manual. We also offer comprehensive training to help you become fully accustomed and pleased with your purchase. Please contact PTI Integrated Systems at (800) 331-6224 to arrange training for your site. If you have any difficulties, we strongly recommend that you review this manual prior to contacting PTI Technical Support.

Using This Manual

This manual is designed to be followed from start to finish for the installation. Operation of the StorLogix Access Control Software is covered in the StorLogix Operations Manual.

There is a Glossary in the back of the manual to define terms that may not be understood. In addition to this, the Index can help you to locate more information about specific topics.

Throughout this manual, there are graphics with cautions, things to remember, hints, and suggested applications. Watch for these as they will help make the installation experience better.



Product Overview

StorLogix access control software as part of the Falcon XT access control system offers a highly customizable security and access control solution for self storage and other rented unit facility operators such as mailbox facilities, locker rentals, parking, etc. StorLogix and Falcon XT are scalable to meet the needs of single site operators to large corporations with hundreds or thousands of sites. With all of the more features and customization, StorLogix has what you need. Security without limits.

Key Features:

- **Digital Video Integration** – allows video to be directly linked to specific areas and events. No need to search through hours of video to find an event, just click on the event in the StorLogix Event Log and the video from that location and time appears on the screen. Video can be monitored at the site as well as over the internet allowing owners to check up on individual sites.
- **PayXpress** – Increase late rental collection and make it easier on your customers and your employees. PayXpress allows customers to pay their late rent at the entry keypad for their convenience and the system will lock them out until they pay for your protection. PayXpress is live credit card processing, so if the card is declined, access can be denied. Late customers don't get in till you get your money. Best of all, it can increase the amount of late fees collected as PayXpress automatically charges the fees in addition to the rent and the customer never gets a chance to talk an employee into waiving the fee. This feature is only available with the purchase of TaskMaster Management Software and necessary Credit Card Processing module and equipment.
- **TaskMaster Integration** – PTI TaskMaster Management Software fully and seamlessly integrates with StorLogix allowing the manager to use one program to manage the money and the access control. New customers in TaskMaster are automatically added to the access control system. This prevents double entry work and makes manager training easier.
- **LogixScript** – Have you ever bought a system that had everything you want, but there was just that 'one more little thing' that you wish it did? Well here it is. If there a custom function for the site that you can't do any other way, LogixScript is here to help. LogixScript allows just about any custom 'If, Then' function to be programmed into the system. Many custom functions can be setup this way.

Other Major Features

- **Management Interface** – StorLogix software can easily be interfaced to any of more than twenty Self Storage management softwares. This allows unit activity such as payments, rentals, and lockouts to be performed from a management software and automatically be updated in StorLogix.
- **Setup Wizards** – Whether doing a basic setup for a small facility or a complicated advanced site for a large multi-location company, the easy to use Setup Wizards will take you step by step through the process.
- **Custom Messages** – Tell your clients that you sell boxes. Let your customers know about referral specials. Remind your employees about the meeting next week. Inform Mr. Jones that his package has arrived at the office. Custom messages allow you to display messages at the keypad for everyone, for groups of people, or for individuals as they enter their code.
- **Customizable Access Areas** – keep individuals or classifications of people out of restricted areas, monitor their movement throughout a site, or just control access onto and off of a site.
- **Customizable Time Schedules** – control the hours that individuals or classifications of people can access the site or specific areas of the site. These can also control for specific situations, such as not allowing customers on the site until an employee has logged onto the site or not allowing employees to enter the office until a manager has logged into that area for the day.
- **Customizable Access Levels** – Groups of users can be created with similar access privileges, such “Managers”, “Maintenance”, or “24-Hour Customers”. This makes is much easier to setup common users without having to remember all of the custom settings for that type of user. These Access Levels can be anything that you want and are completely customizable. Individual users can still be setup with special privileges and access separate from the Access Levels.

Specifications

Workstations	Unlimited
DVR Integration	Optional
Alarm/Monitor Alerts	Phone, email, screen
Custom IO Scripting	LogixScript Included
Lighting Controls	Included – 255 areas per Falcon XT
Access Interface Devices	1 – 127 per Falcon XT
Cards	20,000 per Falcon XT
Users	10,000 per Falcon XT
Custom Messages	700
Access Areas	255 per Falcon XT
Output Points	8,000
Input Points	10,000 per Falcon XT
Time Schedules	255 per Falcon XT
Time Slots	4,096 per Falcon XT
Elevator Controls	64 Elevators 1,024 Floors
Event Filters	Included
Photo ID Badging	Included
Wiegand Formats	4, Custom Available
Access Levels	Yes
Communications	RS232, RS485, RS422, TCP/IP, USB, 900 Mhz 2-way Wireless
Microsoft .Net	Yes
Microsoft SQL, MSDE	Yes

CHAPTER 1: PRE-INSTALLATION

- **INSTALLATION RECOM M ENDATION**
- **TRAINING RECOM M ENDATION**
- **SYSTEM REQUIREM ENTS FOR STORLOGIX**
- **COM PUTER REQUIREM ENTS**
- **OTHER REQUIREM ENTS**
- **PRE-INSTALLATION WORKSHEET**

Review the following pre-installation information and complete the pre-installation worksheet to help make the actual installation process easier. It is strongly recommended that the computer be purchased new, especially for the StorLogix software in accordance with the computer requirements located in this chapter.

Installation Recommendation



While StorLogix and the Falcon XT are intended to be easy to use, the initial installation and setup should be done by a knowledgeable and trained electronics and computer technician. The construction and installation techniques for wiring and installing electronics and the knowledge of applicable codes requires a degree of technical expertise and training that only comes with education and experience. PTI Integrated Systems can recommend local dealers and installers, but it is up to the customer to verify their qualifications and negotiate any pricing or contracts unless PTI has been specifically contracted in writing to do so for the customer.

Training Recommendation



PTI offers comprehensive training for every level of user. PTI strongly recommends that every site take advantage of this training to help each user become familiar with the program. This training can be customized to your site's specific needs in classrooms at PTI Headquarters or on-site at the facility. Contact PTI Technical Support for more information or you can view training information and request training on our web site at www.ptisecurity.com/forms/training.aspx.

System Requirements for StorLogix

StorLogix and the Falcon XT access control system is designed to be easy to implement for small properties with few additional items to purchase, while being fully scaleable for large properties and multiple sites.

1. Installed and working Falcon XT Access Control device
2. Minimum of one installed AI Device or door controller connected to the Falcon XT
3. Computer that meets or exceeds the computer requirements on the following pages.



Computer Requirements

These computer requirements are the minimum for running StorLogix by itself. There are additional requirements for some of the modules and features that can be found on the following pages and for any other software that is added.

1. If you are using any other software along with ours, it is imperative that you make sure that your computer specifications more than exceed the combined total requirements for all of the software that is loaded on the computer.

2. Pentium III or 4, 1.4GHz or higher processor

3. Microsoft Windows 2000 Professional Edition or Windows XP Professional Edition - Service Pack 2 is required

4. 512 MB RAM or higher

5. 20 GB or larger hard drive with 4+ GB available hard drive space

6. CD ROM with a CD-RW, DVD-RW, or Iomega Zip drive for backups

7. SVGA or higher resolution graphics, 1024 x 768 resolution

8. A minimum of a 17" SVGA monitor or better is recommended

9. Sound card and speakers

10. Two or more available working ports (9-pin serial communications port(s), USB port(s), or Ethernet TCP/IP port(s))

11. Broadband/high-speed business internet connection strongly recommended (cable, T1, or DSL)

12. Keyboard & Mouse

13. A high quality Laserjet or Inkjet printer

14. Symantec pcAnywhere host software version 10.5 or higher (PTI Part # PSFT-PCANYWHERE). To receive technical support, you MUST have pcAnywhere. In some cases, Office XP Remote Assistance can be used.



???????? HINT

Take a copy of these requirements to a local computer store along with the requirements for any other software that will be on the computer and have them provide a computer that meets the site's needs.



CAUTION

Do NOT try to use Windows 95, 98, or ME as the operating system on the StorLogix Computer.

15. An updated, working Anti-Virus software such as McAfee Virus Scan, Symantec's Norton Antivirus or other major brand. If the computer will be attached to the internet, especially through broadband connections, a working firewall is recommended. This should be setup by a knowledgeable computer tech because some configuration of this will be required if using pcAnywhere or if StorLogix is networked.
16. UPS (Uninterruptible Power Supply) power backup and surge protection is recommended. (PTI Part # PPWR-UPS-APCBP350US).

**REMEMBER**

Remember to purchase a computer that meets or exceeds the requirements for ALL of the software that will be loaded on it.

**???????? HINT**

For best performance, be sure to have all necessary Windows updates loaded onto the computer before beginning the installation. It is also a good idea to regularly check for Windows updates as well as updates for StorLogix and other programs on the computer.

Other Requirements for StorLogix

Some modules and features require additional items to function. These items may need to be purchased separately.

DVR Integration

- GE or Panasonic Digital Video Recorder purchased from PTI

TaskMaster Integration

- TaskMaster Management Software purchased from PTI

PayXpress

- TaskMaster Management Software with PayXpress module
- TaskMaster Credit Card Module
- High Speed Internet with always online connection & static IP
- PTI Apex Series Keypads version 1.57 or higher with card swipe
- You must have a current account with Nova or Paymentech.

Camera Module

- TWAIN Compatible Internet camera (PTI Part # RTAS-PHOTO-CAMERA). Camera resolution must be approximately 320 x 240

Management Interface

- Management Software that is compatible with PTI's Universal Gate Interface. User must purchase gate interface option from the Management Software company.

Proximity Cards / Photo ID Badges / Swipe Cards

- Compatible wiegand interface cards for Proximity devices
- Any 4 line magnetic stripe card for use with swipe reader devices
- Preprogrammed blank or logo-imprinted cards can be purchased from PTI for either device type.



REMEMBER

These additional requirements are only if the site will be using these additional optional modules and features.



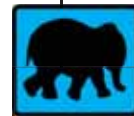
Pre-Installation Worksheet

Complete the worksheet over the following pages to help with the initial loading and setup of the StorLogix software. The information contained in this worksheet will be used when completing the initial setup wizards. Refer to the Glossary in the Appendix of this manual for explanation of any terms or fields.

Company Data

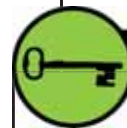
This is the general data about the site itself that is used for the general setup and may appear on various reports.

Site Code	
Company Name	
Address 1	
Address 2	
City	
State	
Postal Code	
Region	
Country	
Phone	
Fax	
Email	
Web Site	
Installer Company	
Installer Contact	
Installer Phone	
Install Date	
Site Administrator Name	
Site Administrator Password	



REMEMBER

More information can be found about any terms or fields in the Glossary in the Appendix of the manual.

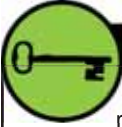


????????? HINT

Site Code and Region are optional fields that can help identify individual sites when a company has multiple sites in StorLogix.

Security Levels

These are the various preset levels of access for the computer operators, including which functions in StorLogix they have access to. StorLogix comes with three default security levels: Administrator, Manager, and Assistant Manager. Complete one of the tables below for each security level desired. Copy this page if more than three are needed.



???????? HINT

It is a good idea to review the existing default Security Levels in StorLogix and customize those to the site before adding new ones. Refer to the General Setup section of this manual for more information on Security Levels.

Security Level Name	
Software Functions NOT allowed for Operators with this Security Level	

Security Level Name	
Software Functions NOT allowed for Operators with this Security Level	

Security Level Name	
Software Functions NOT allowed for Operators with this Security Level	

Time Schedules

Time Schedules generally are preset hours that users and operators are allowed on the site. StorLogix comes with two default Time Schedules: 6 am – 6 pm and 24 hour. Each Time Schedule includes the days of the week and holidays as well as any hours of access during the day or night, broken up into Time Slots, which are units of time during which access is allowed. Each Falcon XT can support up to 255 time schedules with up to 4096 time slots. Complete one of the tables below for each Time Schedule desired. Copy this page if more are needed.

Time Schedule Name	
Days Access Allowed	<input type="radio"/> Mon <input type="radio"/> Tue <input type="radio"/> Wed <input type="radio"/> Thu <input type="radio"/> Fri <input type="radio"/> Sat <input type="radio"/> Sun <input type="radio"/> Holidays
Hours Access Allowed for Each Day	

Time Schedule Name	
Days Access Allowed	<input type="radio"/> Mon <input type="radio"/> Tue <input type="radio"/> Wed <input type="radio"/> Thu <input type="radio"/> Fri <input type="radio"/> Sat <input type="radio"/> Sun <input type="radio"/> Holidays
Hours Access Allowed for Each Day	



APPLICATION

Time Schedules are used by many other functions in the program including Holidays, Lighting Areas, Access Levels, and others. They can also be used with LogixScript to setup many custom functions. Refer to these sections of the manual for more information.

AI Devices

AI Devices, including Keypads, Card Readers, Multiplexers, Relay Boards, and Wiegand devices must be setup in StorLogix. It is a good idea to have a sketch of the site showing each device, what its address is, what its functions are, and what it is connected to. Each Falcon XT can support up to 127 of these devices. Copy this page and complete one for each AI Device on the site.

AI Device Type	
AI Device ID / Address	
Location On-site	
If Device is Keypad/Wiegand What Door/Gate does it open? What are its other functions (if any)? What is Relay # 1 connected to? What is Relay # 2 connected to? What Access Area does it enter/exit from? What Access Area does it enter/exit to?	
If Device is a Multiplexer Is it Hardwired or Wireless? How many channels does it have? How many channels are used? What Building(s) is it for? What doors/alarm devices does it monitor? Does it have an Auxiliary Siren? What Alarm Zone is it in?	
If Device is a Relay Board How many relays are used? What is each relay connected to? Are there any door inputs used? What is the purpose of each relay?	



REMEMBER

Relays can be used to open or close gates/doors, activate sirens, control lights, control elevator buttons, or hold for certain LogixScript custom functions.

Alarm Zones

Alarm Zones allow a site with multiple sirens to create areas or zones where the sirens sound only for alarms that occur in that area. StorLogix has one default alarm zone, called the Global Alarm Area, which is setup to sound any auxiliary siren when any alarm is triggered. Complete one of the tables below for each Alarm Zone on the site. Copy this page if more than four are required.

Alarm Zone Name	
Start Time - Day	
On Time - Day	
Start Time - Night	
On Time - Night	
Relays to trip for this Zone	

Alarm Zone Name	
Start Time - Day	
On Time - Day	
Start Time - Night	
On Time - Night	
Relays to trip for this Zone	

Alarm Zone Name	
Start Time - Day	
On Time - Day	
Start Time - Night	
On Time - Night	
Relays to trip for this Zone	

Alarm Zone Name	
Start Time - Day	
On Time - Day	
Start Time - Night	
On Time - Night	
Relays to trip for this Zone	



APPLICATION

Sirens connected to Multiplexer Auxiliary relays or to Apex Keypads using Relay # 2 set to Alarm Output will sound only as part of the Global Alarm Area.

Additional Alarm Area sirens must be connected to relays on the Falcon XT, Relay Boards, or Apex Keypads using Relay # 2 set to Aux Output. Unused relays in other keypad devices may be used for this also.

Lighting Areas

Lighting areas are relays connected to lights in hallways, stairwells, building exteriors, or units that are set to come on for certain users entering that access area. Complete a table for each lighting area. Copy this page if more than six lighting areas are needed.

Lighting Area Name	
Relays to Trip (AI Device and Relay #)	
Location (Building or Access Area)	
Is this a Pass Through Lighting Area	

Lighting Area Name	
Relays to Trip (AI Device and Relay #)	
Location (Building or Access Area)	
Is this a Pass Through Lighting Area	

Lighting Area Name	
Relays to Trip (AI Device and Relay #)	
Location (Building or Access Area)	
Is this a Pass Through Lighting Area	

Lighting Area Name	
Relays to Trip (AI Device and Relay #)	
Location (Building or Access Area)	
Is this a Pass Through Lighting Area	

Lighting Area Name	
Relays to Trip (AI Device and Relay #)	
Location (Building or Access Area)	
Is this a Pass Through Lighting Area	

Lighting Area Name	
Relays to Trip (AI Device and Relay #)	
Location (Building or Access Area)	
Is this a Pass Through Lighting Area	



APPLICATION

Lighting areas are most often used to save money on power bills by leaving the lights turned off for a building or area when no one is in the area and turning them on when a user with a unit in that area comes on the site. This could also be used to turn on a safety exhaust fan whenever someone enters an area that requires circulation.

Lighting Areas are really just area specific relays that can be used for many things such as climate controls based on Time Schedules to turn air conditioning or heating just before business hours and turning them down or back off after business hours to save money. They can also be used to turn on lighted signs or exterior building lights at night.

Building Setup

Building setup is used for Lighting Areas, Access Areas, and Elevator Zones. Each building is given a name (A, B, C, 1, 2, 3, Main, etc). Complete a table below for each building on the site. Copy this page if more than ten are needed.

Building Name	
Number of Floors	

Building Name	
Number of Floors	

Building Name	
Number of Floors	

Building Name	
Number of Floors	

Building Name	
Number of Floors	

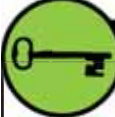
Building Name	
Number of Floors	

Building Name	
Number of Floors	

Building Name	
Number of Floors	

Building Name	
Number of Floors	

Building Name	
Number of Floors	



???????? HINT

Building Setup is not necessary if the individual buildings on a site do NOT have their own keypad or door controller, Lighting Areas, or Access Areas.

Elevator Setup

Elevator Setup is only used if the elevators are controlled by the StorLogix and Falcon XT Access Control System. Complete one of the tables below for each elevator. If more than five are needed, copy this page.


Elevator Name	
Building that Elevator is in	
Lowest Floor Number	
Highest Floor Number	
Relays Triggered	

Elevator Name	
Building that Elevator is in	
Lowest Floor Number	
Highest Floor Number	
Relays Triggered	

Elevator Name	
Building that Elevator is in	
Lowest Floor Number	
Highest Floor Number	
Relays Triggered	

Elevator Name	
Building that Elevator is in	
Lowest Floor Number	
Highest Floor Number	
Relays Triggered	

Elevator Name	
Building that Elevator is in	
Lowest Floor Number	
Highest Floor Number	
Relays Triggered	



???????? HINT
 Elevator Control Setup can be very complicated. It is a good idea to read the Elevator Setup section of this manual prior to beginning this process.

Access Areas

Access Areas are parts of the site where access is controlled by keypads or Wiegand devices. Access Areas can be inside other Access Areas, buildings, etc. For example, most sites will have a Default Access Area that is the entire site inside the fence line. Within that access area may be several buildings, each with their own keypads for access. Inside each building may be several floors, each with their own keypads for access. Inside each floor may be several rooms, each with their own keypads for access. Complete a table below for each access area on the site. If more than six access areas are needed, copy this page.

Access Area Name	
Building	
Floor	

Access Area Name	
Building	
Floor	

Access Area Name	
Building	
Floor	

Access Area Name	
Building	
Floor	

Access Area Name	
Building	
Floor	

Access Area Name	
Building	
Floor	



???????? HINT

If the site only has keypad access control on a gate at the fence line and does not have individual keypads controlling access to buildings or areas inside the site, then Access Areas will not need to be setup as the default area will cover the whole site.



APPLICATION

Access Areas can be used to keep unauthorized users out of areas where they do not belong or they can be used just to monitor where users go within a site.

Access Levels

Access Levels are used to add groups of people with similar access privileges. For example, if a site has several managers, several employees, and customers with two different types of access, they can setup access levels to make it easier to add each of these types of users without having to remember all of the variables every time one is added. Access Levels are a combination of Access Areas and Time Schedules. Complete a table below for each access level to be used. If more than five access levels are needed, copy this page.

Access Level Description	
Required Level On-site	
Access Area	
Time Schedule	

Access Level Description	
Required Level On-site	
Access Area	
Time Schedule	

Access Level Description	
Required Level On-site	
Access Area	
Time Schedule	

Access Level Description	
Required Level On-site	
Access Area	
Time Schedule	

Access Level Description	
Required Level On-site	
Access Area	
Time Schedule	



APPLICATION

Access Levels can also be used to keep employees out of the office when a manager is not in the area or to keep clients out of a building until an employee is on-site.

Setup Operators

Operators are users that have access to the StorLogix software on the computer. During the initial site setup, one Administrative Operator is created along with a default Administrator. Other users with different Security Levels can be created and added later. If more than five are required during initial setup, make additional copies of this page.

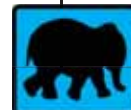
Operator Name (First & Last)	
Operator Login Name	
Operator Password	
Security Level	

Operator Name (First & Last)	
Operator Login Name	
Operator Password	
Security Level	

Operator Name (First & Last)	
Operator Login Name	
Operator Password	
Security Level	

Operator Name (First & Last)	
Operator Login Name	
Operator Password	
Security Level	

Operator Name (First & Last)	
Operator Login Name	
Operator Password	
Security Level	



REMEMBER

Users have access to the site (customers and employees). Operators are users (usually employees) that have access to the StorLogix software.

Setup Falcon XT

These are miscellaneous settings for the Falcon XT.

AI Devices Baud Rate	
Host Computer Baud Rate	
Log Off Time of Day	<input type="radio"/> None <input type="radio"/> Time _____
Undefined Input Reporting	<input type="radio"/> Yes <input type="radio"/> No
Undefined Tamper Reporting	<input type="radio"/> Yes <input type="radio"/> No
Undefined Check-In Reporting	<input type="radio"/> Yes <input type="radio"/> No
Unknown Battery Change Reporting	<input type="radio"/> Yes <input type="radio"/> No
Use Facility Code (Prox Cards)	<input type="radio"/> Yes <input type="radio"/> No
Entire Alarm System On	<input type="radio"/> Yes <input type="radio"/> No
Vacant Alarms On	<input type="radio"/> Yes <input type="radio"/> No
Communication Alarms On	<input type="radio"/> Yes <input type="radio"/> No
Allow Exit with Door Open	<input type="radio"/> Yes <input type="radio"/> No



REMEMBER

The Baud Rate programmed in StorLogix for the AI Devices must match the actual Baud Rate programmed at each AI Device and all AI Devices must have the same Baud Rate.

The Baud Rate for the Host Computer programmed in StorLogix must match the Baud Rate set in the Device Manager on the computer.

The AI Device Baud Rate and the Host Computer Baud Rate do NOT have to match each other.

Setup DVR


The DVR can be integrated with StorLogix, so that clicking on an event in the Event Log history will bring up the video with the most relevant camera view for that event. Each camera can be tied to various inputs (door alarms), relays, and specific AI devices.

DVR Description	
DVR Brand/Model	
DVR IP Address	
DVR Password	

Setup Cameras

Each camera can have multiple devices, inputs, and relays associated with it. If there are more than 16 cameras on the site, make additional copies of this page.

Camera Number	AI Devices to Camera Device ID	Relays to Camera Device ID & Relay #	Inputs to Camera Mux ID & Channel #
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			



APPLICATION

By using a DVR compatible with StorLogix, events can be associated with recorded camera footage.

Each AI Device, Input, and Relay can be associated with the nearest camera or cameras. With proper site security planning, this will make it easy to find and review the video for an event.

For Example: if the site has a camera pointed at the entrance gate, a second camera pointed at the license plate area of a car, and a final pinhole camera in the keypad; then every time a user enters the site, the site manager can view the video of the user's car, license plate, and face with a single click on a single event.

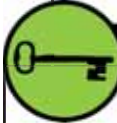
A site that has a hallway of doors, each with a door alarm switch, can associate all of the switches (inputs) with a camera pointed down the hall to allow the manager to immediately view the footage of that hallway if an alarm goes off in that area.

Relays can also be associated with a camera. This could be used to associate a camera pointed at an elevator (or inside the elevator car) to the elevator relay button being activated.

Setup Holidays

Holidays can be used to set specific days during the year when business hours or access hours change, restricting access or closing it off altogether. Use this table to fill in any holidays for the site. If more than twenty holidays are needed, make additional copies of this page. Holidays are not required for a site.

Holiday Name & Date	Holiday Start Time	Holiday End Time	Affected Time Schedules



???????? HINT

Holidays are only used if a site has different business hours on holidays or is closed. The actual authorized holiday hours are setup individually for each Time Schedule.

This could be used to allow employee access to a site during a holiday while preventing customer access.

Chapter Terms

Access Area	Parts of the site where access is controlled by keypads or Wiegand devices. Access Areas can be inside other Access Areas. For example, most sites will have a Default Access Area that is the entire site inside the fence line. Within that access area may be several buildings, each with their own keypads for access. Inside each building may be several floors, each with their own keypads for access. Inside each floor may be several rooms, each with their own keypads for access. These would all be access areas.
Access Level	Used to add groups of people with similar access privileges. For example, if a site has managers, employees, and customers with two different types of access, they can setup access levels to make it easier to add each of these types of users without having to remember all of the variables every time one is added. Access Levels are a combination of Access Areas and Time Schedules.
Address	The site's street number name when entering site setup information. Also, another name for AI Device ID in connection with previous Falcon Systems.
Administrator	User with full rights to setup or change any part of StorLogix.
AI Device	Any Keypad, Multiplexer, Relay Board, or Wiegand device. In previous Falcon Systems, this was referred to as a Remote.
AI Device ID	The unique identifier number programmed in to each AI Device to differentiate it from other AI Devices when communicating to the Falcon XT. Referred to as Address in previous Falcon Systems.
AI Device to Camera	To associate an AI Device to a specific camera to allow any events from that device to show the video from that camera at that time when the event is clicked on.
AI Devices Baud Rate	Communications speed between the AI Devices and the Falcon XT. This is programmed at each AI Device AND in StorLogix and must match between all of them.
Alarm Zone	These allow a site with multiple sirens to create areas or zones where the sirens sound only for alarms that occur in that area.
Allow Exit with Door Open	If a unit door has an alarm switch on it, this setting can be turned on to remind the user that the door to their unit was not closed.
Anti-Virus	Software that helps protect the computer from viruses.
Auxiliary Siren	A siren connection on multiplexers that will sound the siren if any alarm occurs on the site.
Baud Rate	Communications speed between devices. See AI Device Baud Rate and Host Computer Baud Rate.
Building	For the purposes of StorLogix, any structure on a site that has its own keypad or door controller to monitor or control access.
Channel	An individual alarm input point on a multiplexer, APEX keypad, 8-channel relay board, or Falcon XT.
Communication Alarms	Alarm events in StorLogix that may sound the siren if an AI Device stops communicating due to vandalism, poor installation, etc.

Communication Port	A connection point on a computer that allows other devices to be connected to the computer including the Falcon XT.
Door Controller	A Wiegand device or keypad that controls the access to a door.
Door Input	An alarm input point for door contacts
DVR	Digital Video Recorder.
DVR Integration	Allows a compatible DVR to be connected with StorLogix so that events can be associated with cameras making video quick and easy to locate.
Elevator Control	Using Relay Boards, StorLogix can be programmed to prevent users from getting to floors in a building that they should not have access to. When the user enters their code at an elevator keypad, only the button to the floor with their unit will light.
Entire Alarm System On	This is a function in the Falcon XT setup that allows the entire alarm system to be turned off by deselecting this check box. Generally, this would only be done for maintenance or troubleshooting purposes.
Ethernet	A type of network setup for computers to allow multiple computers to be connected together.
Falcon XT	Controller for AI Devices programmed and operated using StorLogix.
Floor 1	The lowest floor on a site. This is not always the ground floor. Sites with sublevels or basements that the elevator accesses will have Floor 1 as the lowest subfloor serviced by the elevator.
Highest Floor Number	The highest floor that an individual elevator actually services. This becomes very important in high rise buildings where some elevators only service certain floors.
Holidays	A program setting in StorLogix that allows the regular access hours to change or be locked out on certain days of the year.
Holiday End Time	The actual time during the day on a holiday date when the Holiday hours end. This allows regular access to resume after this time.
Holiday Start Time	The actual time during the day on a holiday date when the Holiday hours begin. Regular access hours are active until this time.
Host Computer Baud Rate	The communications speed between the StorLogix computer and the Falcon XT. This baud rate is set in StorLogix and must match in the Windows Device Manager.
Input	A point in the system that alarm switches, motion sensors, glass break sensors, door contacts, or tamper switches can be connected.
Input to Camera	To associate an input to a specific camera to allow any events from that input to show the video from that camera at that time when the event is clicked on.
IP Address	A unique identifier number assigned to computers on a network to differentiate them from each other.
Lighting Area	Lighting areas are relays connected to lights in hallways, stairwells, building exteriors, or units that are set to come on for certain users entering that access area.
Log Off Time of Day	Optional setting that clears all users off the site at a certain time every day to remove users that may have tailgated off the site from the access. This should not be used on-sites with 24 hour access.

Lowest Floor Number	The lowest floor that an individual elevator actually services. This becomes very important in high rise buildings where some elevators only service certain floors.
Management Software	Software used to manage a site. In self storage, these programs are used to rent units, send letters, assess fees, sell merchandise, and track the collections and auction process.
Multiplexer OR Mux	An AI Device used to combine multiple input signals into one output data signal. It is a connection point for door alarms that feeds the information from multiple doors back to the Falcon XT.
Mux ID	The AI Device ID for a Multiplexer programmed using the switches on the multiplexer circuit board.
Nova	One of the two Credit Card Processing companies that can be used with PayXpress. See Also Paymentech.
On Time – Day On Time – Night	The length of time that a lighting zone or alarm zone siren will stay on for if activated during Daytime or Nighttime hours.
Operator	A User that has access to the StorLogix software. Generally an employee of the site.
Paymentech	One of the two Credit Card Processing companies that can be used with PayXpress. See Also Nova.
PayXpress	Module in TaskMaster and StorLogix that allows credit card payments to be made from an APEX mag-stripekeypad so customers can pay at the gate.
pcAnywhere	A software program by Symantec that allows one computer to 'dial in' to another computer and control it. Generally used for technical support and for home office control of remote sites.
Region	An optional field in StorLogix to identify the site when a single company owns multiple sites. (i.e. Southwest, Pacific, Asian, etc).
Relay	A switch located in electronics used to control another device.
Relay Board	An AI Device that has two or more relays used to control other electronics such as gates, doors, lights, elevators, sirens, etc.
Relay to Camera	To associate a relay to a specific camera to allow any events from that relay to show the video from that camera at that time when the event is clicked on.
Remote Assistance	Windows XP function that allows one computer to 'dial in' to another computer and control it. Generally used for technical support and for home office control of remote sites.
Required Level On-Site	An Access Level setting used to prevent one group of users from entering the site until a person from another group has logged onto the site. For example, customers could be locked out of a site until an employee is there or employees could be locked out of an office or warehouse area until a manager is present.
Security Level	These are the various preset levels of access for the computer operators, including which functions in StorLogix they have access to.
Serial Port	A 9-pin communications port using RS232 communications. One of the three ways that the Falcon XT can be connected to the StorLogix computer.

Site Code	An optional four digit identifier that can be used to identify individual sites when a company owns multiple sites. Many companies have store numbers that this could be used for.
Start Time – Day	This is the beginning of daytime hours for a site for use with alarm zones and lighting areas. This allows the site to set their daytime hours to whatever they need to meet individual site needs or local code restrictions on alarm sirens.
Start Time – Night	This is the beginning of nighttime hours for a site for use with alarm zones and lighting areas. This allows the site to set their nighttime hours to whatever they need to meet individual site needs or local code restrictions on alarm sirens.
SVGA	Super Video Graphics Array. A graphics monitor display standard.
TCP/IP	A protocol for computer networks.
Time Schedule	Time schedules generally are preset hours that users and operators are allowed on the site, but can also be used to control time for other functions such as Holidays, Lighting Areas, and many custom LogixScript functions.
Undefined Check-In Reporting	An optional setting in the Falcon XT setup that allows the system to display or ignore check-in events for devices that are undefined in the system.
Undefined Input Reporting	An optional setting in the Falcon XT setup that allows the system to display or ignore events for inputs that are undefined in the system.
Undefined Tamper Reporting	An optional setting in the Falcon XT setup that allows the system to display or ignore events for tamper switches that are undefined in the system.
Unit	Units are storage spaces, rooms, offices, mailboxes, lockers, parking spaces, and other areas that are generally rented to clients. However, they can include manager units, storage sheds, dumpster areas, security closets, and any other enclosed area that might be monitored.
Unknown Battery Change Reporting	An optional setting in the Falcon XT setup that allows the system to display or ignore device battery change events for devices that are undefined in the system.
UPS	Uninterruptible Power Supply – A device that provides high level surge protection, battery backup, and power conditioning for electronics devices.
USB	Universal Serial Bus. A communications protocol. One of the three ways that the Falcon XT can be connected to the StorLogix computer.
Use Facility Code	A code that is used with proximity cards. May shorten all codes if not used.
User	Any person that has access to the site, including customers, managers, employees, and others.
Vacant Alarms	An optional setting in the Falcon XT setup that allows the system to display or ignore alarm events from units that are not rented. This is a good feature to keep turned on to prevent vacant units from being used for criminal purposes.
Virus	A malicious software program that is designed to damage a computer that is generally loaded on the computer without the operators knowledge and runs without permission.

CHAPTER 2: LOADING THE SOFTWARE

- **BEGINNING THE INSTALL**
- **LOADING THE MSDE**
- **LOADING ADOBE READER**
- **LOADING EASY LINK**
- **LOADING STORLOGIX**
- **LOADING LOGIXSERVER**
- **DESKTOP ICONS**
- **DEMONSTRATION MODE**
- **REGISTERING THE SOFTWARE**
- **SOFTWARE ACTIVATION**

StorLogix software actually consists of several different programs that are loaded during the installation process. Some computers may require additional software or updates. Any such additional items will be found during the installation preparation process and will load during the installation process. In most cases, everything that is needed is contained on the StorLogix software CD. Be sure that the Falcon XT is connected to the StorLogix computer and operational before beginning the loading process.

Beginning the Install

Make sure that the Falcon XT is connected to all AI Devices and powered up.

Make sure that the AI Devices all have their AI Device ID's set with no duplicates (refer to the manual for each AI Device for more information on this).

Make sure that the Falcon XT is connected to the StorLogix computer using the enclosed Serial cable, USB cable, or using an Ethernet cable.

Load the StorLogix CD in the CD drive on the computer.

The computer will automatically run the StorLogix installer program.



Figure 2-1: The StorLogix CD

The Installer box will show which programs that need to be installed. Generally, this will be the Microsoft SQL Server Desktop Engine, Adobe Reader, Easy Link, StorLogix, and LogixServer; but, occasionally, there will be other items that are necessary for that computer. Click on **Install** to begin.



Figure 2-2: StorLogix Installer Components Screen. Components shown will be installed. To change this list or to add other components, click on the Advanced button.

???????? HINT

If the StorLogix CD does not automatically run when inserted into the computer, left click on the Start Button on the Start Bar at the bottom of the screen and select 'Run'.

Type in `D:\setup.exe` and then click on the OK button. If the CD drive on the computer is set to something other than 'D' be sure to type that letter instead of 'D'.

REMEMBER

The Falcon XT must be connected to the StorLogix computer and operational with all AI Devices connected prior to beginning the software loading process.

???????? HINT

The installation process shown over the following pages may vary from computer to computer depending on the software previously loaded on it. In some cases additional software and updates will need to be loaded from the StorLogix Installer Components - Advanced button or from various other sources including the Microsoft Windows and Microsoft Office installation CD's and some internet sources.

Loading the MSDE

The Microsoft SQL Server Desktop Engine (MSDE) is the database engine used by StorLogix. This is the first item installed.

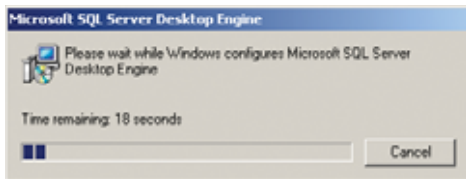


Figure 2-3: MSDE Loading Screen

When the MSDE has been installed, a dialog box will appear. Click **OK** to continue.



Figure 2-4: MSDE Successfully Loaded

At this point, the computer will need to be restarted. This must be done before the installation can be completed. Click **Yes** to continue. After the computer restarts, the installation process will automatically continue.



Figure 2-5: Restart Computer

Loading Adobe Reader

After the computer restarts, Adobe Reader should begin loading. Adobe Reader is used to read .pdf documents such as Manuals, web downloads, and other documentation.



Figure 2-6: Adobe Reader Install automatically begins.

When the Adobe Reader installation screen comes up, click on **Next** to continue the installation.

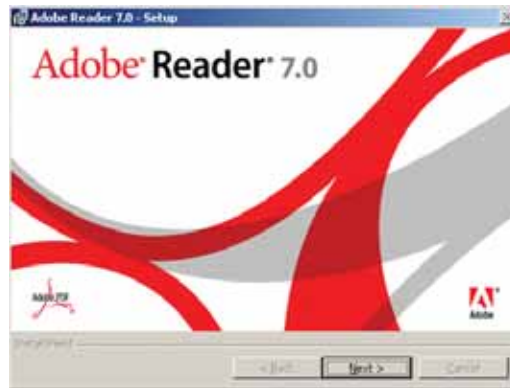


Figure 2-7: The Adobe Reader Installation Setup splash screen.

???????? HINT

If you already have Adobe 6.0 or higher on the computer, there is no need to load Adobe Reader 7.0. This program is useful to have, not only for PTI products, but many other web sites and companies put their documentation in Adobe .pdf files.

Click on **Next** to begin installing Adobe Reader on the computer.



Figure 2-8: The Adobe Reader Setup Wizard screen 1.

Adobe will automatically select a destination folder for the installation. To change this destination folder, click on the **Change Destination Folder** button. In most cases, it is better to leave the installation folder as the default. Click **Next** to continue.



Figure 2-9: Choosing a Destination Folder for Adobe

To begin installing the program in the selected folder, click on the **Install** button.

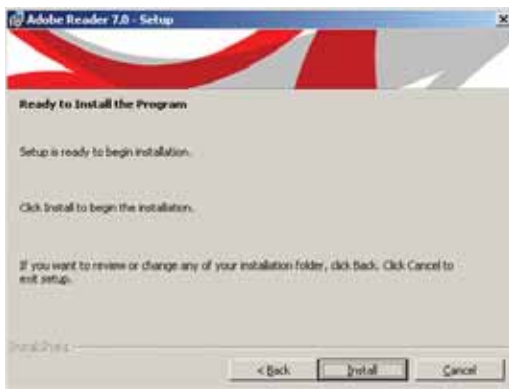


Figure 2-10: Begin the Adobe install

Adobe Reader will begin installing on the computer. This may take a few minutes.



Figure 2-11: Adobe Install in process

When the Adobe Reader installation process is finished, click on the **Finish** button.

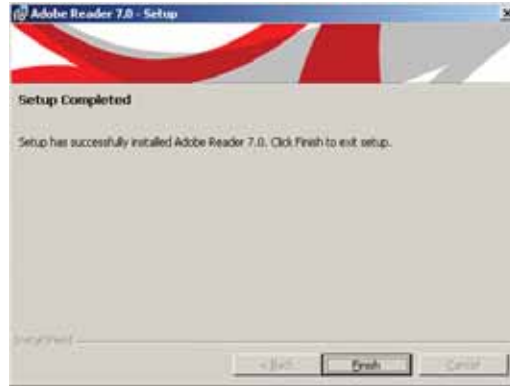


Figure 2-12: Adobe Install processed finished

A dialog box will appear. Click **OK** to continue.

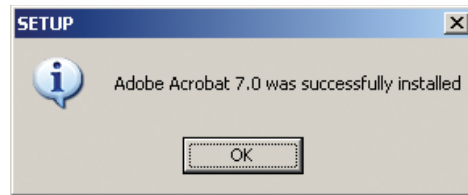


Figure 2-13: Adobe Install successfully completed

Loading Easy Link

The next software to load is the Easy Link program. The Easy Link program is used to interface StorLogix to many types of management software. All other programs must be closed before beginning this install. Close all other programs and then click on the **Yes** button to continue.



Figure 2-14: Easy Link Install warning to close all other programs.

The Easy Link splash screen will appear. Click **Next** to begin the installation setup process.



Figure 2-15: Easy Link Install splash screen.

Enter the Name and Company Name of the person that will be registered as the software owner. Click **Next** to continue.

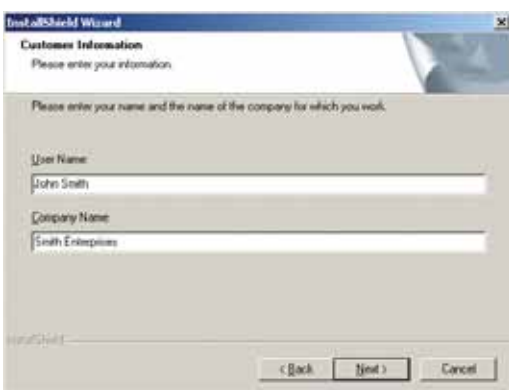


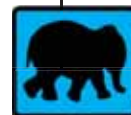
Figure 2-16: Easy Link customer information screen.



APPLICATION

Easy Link is used to interface StorLogix with many types of Management Software other than PTI TaskMaster. PTI TaskMaster directly integrates with StorLogix offering functions and features not available with other Management Software.

The interface allows client functions such as renting units, suspending access due to non-payment, etc. to automatically download the result to StorLogix. Therefore, a new tenant is only entered in the Management Software, which automatically downloads into StorLogix preventing double work for the manager. Also, customers who are locked out due to non-payment have their access automatically suspended to help prevent them from removing their things from the unit until the site gets paid.



REMEMBER

In most cases, the site must also purchase the gate interface option from the management software company. They often charge a fee for the ability to interface to the access control system. Contact the management software company for more information on this.

If the site has TaskMaster and StorLogix, PTI does not charge for the interface. If the site has StorLogix and another management software, then PTI does not charge for the interface, but the management software company may.

Click on the **Next** button to begin the actual installation of the software.



Figure 2-17: Start the Easy Link Install

The Easy Link software will begin loading on the computer. This may take a few minutes. A status bar will show how much of the installation is complete.

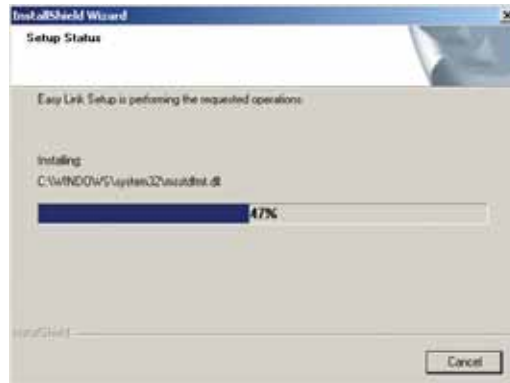


Figure 2-18: Easy Link installation in process.

When the installation is complete, click on the **Finish** button to exit the install wizard.

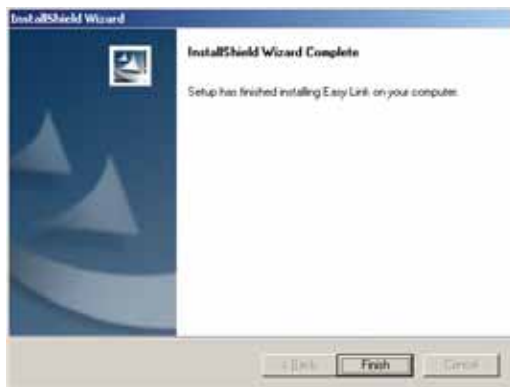


Figure 2-19: Easy Link install complete

A dialog box will appear. Click **OK** to continue.



Figure 2-20: Easy Link was installed successfully

Loading StorLogix

After the Easy Link software loads, the StorLogix software will automatically begin loading.



Figure 2-21: StorLogix software preparing to install

Once the computer has been prepared, the StorLogix Setup Wizard will come up. Click on **Next** to begin the Setup process.




Figure 2-22: StorLogix installation splash screen.

The PTI End User License Agreement (EULA) comes up. Take a moment and read the EULA by scrolling down. The EULA is also available in the appendix of this manual. When you have completed reading the EULA, click on **I Agree** and then the **Next** button. If you do not agree to the terms of the EULA, you cannot install the program.



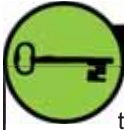
Figure 2-23: StorLogix End User License Agreement - you must click on the I Agree to continue the process.



REMEMBER

The End User License Agreement covers the rights and responsibilities for using the software. A copy of this can be reviewed in the Appendix of this manual.

Select the Installation Folder. In most cases, it is better to leave the installation folder as the default. Also, select **Everyone** to allow any computer users to access StorLogix or **Just Me** if it will only be available for the person who is installing the program. Generally, **Everyone** should have access to the program. Click **Next** to continue.



????????? HINT

Selecting 'Everyone' on this screen doesn't mean that everyone can actually access the software, it only means that they will be able to see the icon on the computer desktop. To actually open and use the software, they will need to have a Login and Password for the program.

If 'Just Me' is selected, then only the person logged onto Windows at the time of installation will ever be able to see the StorLogix Icon.

We recommend that 'Everyone' be selected here.



Figure 2-24: Select the StorLogix Installation Folder screen

At this point, the installation can be reviewed by clicking on **Back** to go back through the steps or click **Next** to confirm the installation and continue.



Figure 2-25: Begin the StorLogix Installation screen

StorLogix will begin installing on the computer. This will take a few minutes to complete. The blue bar in the middle of the window will show the progress. Clicking on **Cancel** will end the installation



Figure 2-26: StorLogix is being Installed screen.

When the installation process has completed, click on **Close**. Be sure to use the Windows Update program on the computer to check for critical updates to the .NET Framework.



Figure 2-27: StorLogix installation complete screen.

If StorLogix was successfully installed, the setup window will pop up. Click **OK** to complete the process.



Figure 2-28: StorLogix was successfully installed.

Loading LogixServer

After StorLogix has been loaded, LogixServer will automatically begin the loading process. LogixServer is the program that controls communication between StorLogix and the Falcon XT.



Figure 2-29: LogixServer preparing to install on the computer

Once the computer has been prepared, the LogixServer Setup Wizard will come up. Click on **Next** to begin the Setup process.



Figure 2-30: LogixServer installation splash screen

The PTI End User License Agreement (EULA) comes up. Take a moment and read the EULA by scrolling down. The EULA is also available in the appendix of this manual. When you have completed reading the EULA, click on **I Agree** and then the **Next** button. If you do not agree to the terms of the EULA, you cannot install the program.



Figure 2-31: LogixServer End User License Agreement - you must click on the I Agree to continue the process.



REMEMBER

The End User License Agreement covers the rights and responsibilities for using the software. A copy of this can be reviewed in the Appendix of this manual.

Select the Installation Folder. In most cases, it is better to leave the installation folder as the default. Also, select **Everyone** to allow any computer users to access LogixServer or **Just Me** if it will only be available for the person who is installing the program. Generally, **Everyone** should have access to the program. Click **Next** to continue.



Figure 2-32: Selecting the LogixServer installation folder

At this point, the installation can be reviewed by clicking on **Back** to go back through the steps or click **Next** to continue.



Figure 2-33: Logix Server installation confirmation screen.

LogixServer will begin installing on the computer. This will take a few minutes to complete. The blue bar in the middle of the window will show the progress. Clicking on **Cancel** will end the installation.



Figure 2-34: LogixServer install in progress screen.

?

HINT

Selecting 'Everyone' on this screen doesn't mean that everyone can actually access the software, it only means that they will be able to see the icon on the computer desktop. To actually open and use the software, they will need to have a Login and Password for the program.

If 'Just Me' is selected, then only the person logged onto Windows at the time of installation will ever be able to see the StorLogix Icon.

We recommend that 'Everyone' be selected here.

When the installation process has completed, click on **Close**.



Figure 2-35: LogixServer installation complete screen.

CAUTION

Be sure to use the Windows updates program on the computer to check for critical updates to the .NET Framework.

If LogixServer was successfully installed, the setup window will pop up. Click **OK** to complete the process.

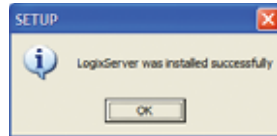


Figure 2-36: LogixServer was installed successfully.

When all installation is complete, seven new icons will be installed on the computer desktop.

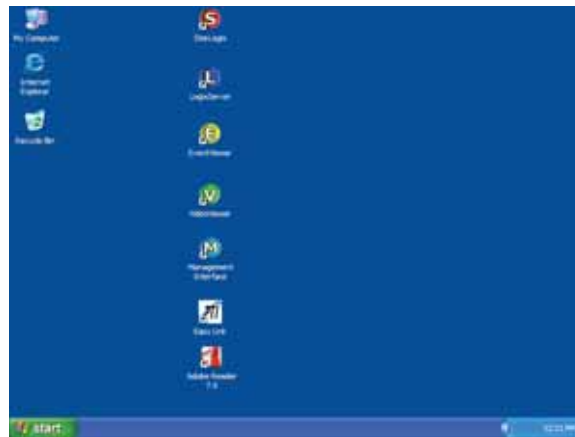


Figure 2-37: Desktop showing all seven new icons.

Desktop Icons

The following icons are installed on the computer desktop during the StorLogix and LogixServer installations.



StorLogix Icon - This icon accesses the StorLogix program, used to control the Falcon XT access control system. This program must be open and running everyday. This is the first icon to click on when beginning to use the software.



LogixServer Icon - This icon accesses the LogixServer program. This program is the communications server that allows StorLogix to communicate with the Falcon XT. Generally, once this is setup, there is no need to go back into this program.



EventViewer Icon - This icon accesses the EventViewer program. This program is used to review the complete history of events in StorLogix and the Falcon XT.



VideoViewer Icon - This icon accesses the VideoViewer program. This program is used to view the video when a Digital Video Recorder is integrated with StorLogix software.



Management Interface Icon - This icon accesses the Management Interface program that allows StorLogix to communicate with TaskMaster management software. Generally, once this is setup, there is no need to go back into this program.



Easy Link Icon - This icon accesses the Management Interface program that allows StorLogix to communicate with various self storage management software programs. Generally, once this is setup, there is no need to go back into this program.



Adobe Reader Icon - This icon accesses the Adobe Reader program that is used to read the Manual files for StorLogix. Generally, there is no need to go into this program. Opening a manual file will automatically open Adobe Reader.



???????? HINT

Once StorLogix is setup and running at the site, the LogixServer, Management Interface, Easy Link, and Adobe Reader icons can be removed from the computer desktop.

Only the StorLogix, EventViewer, and VideoViewer icons will be used on a regular basis.

Demonstration Mode

StorLogix can be run in Demonstration Mode for up to 30 days. This allows a site to test the software functionality prior to purchase.

Double click the StorLogix icon on the computer desktop.



Figure 2-38: StorLogix Icon

The StorLogix licensing window will come up. The number of days remaining in the demonstration period will show at the bottom of the



Figure 2-39: StorLogix Licensing Window

window.

Click on the **Try** button to begin the Demonstration Setup and to view the software.

Each time that StorLogix is used during the 30 day demonstration period, this screen will appear. After 30 days, the software will become inactive and cannot be used without purchasing the software and registering it with PTI.

To register the software at any time, click on the **Register** button.



REMEMBER

There are only 30 calendar days in the Demonstration Mode. After the 30th day, the program will no longer function unless purchased and activated.

Registering the Software

Each time that StorLogix is opened during the Demonstration Period, the StorLogix licensing window will come up. To register the software, click on the Register button.



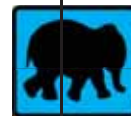
Figure 2-40: StorLogix Licensing Window

Enter the Registration information including the purchaser name and organization. This is very important as this person will be registered as the software purchaser with PTI. When the software is paid for, PTI will provide a Serial Number to enter on this screen. If you do not have this Serial Number, contact PTI to obtain one.



Figure 2-41: StorLogix Registration Information screen

After entering all registration information, click on the **Register** button to continue.



REMEMBER

The only way to get an Activation Serial Number is to purchase the software and contact PTI Technical Support.

Software Activation

After clicking on the Register button, the Activation screen will come up. If the computer has an internet connection, click on **Activate Online** and then the **Continue** button. This will automatically activate the software.



Figure 2-42: StorLogix activation online screen.

If the computer does not have an active internet connection, click on **Activate by Email or Phone** and then click the **Continue** button.



Figure 2-43: StorLogix activation by email or telephone screen.

To activate by Email, click on **Copy to Email**. This will bring up an Outlook or Outlook Express email with the Serial Number and Machine key in it. Include the site name, your name, and a telephone number and send the email to PTI technical support at support@ptisecurity.com. If the email account is not Outlook or Outlook Express, click on the **Copy to Clipboard** button and then paste it into the other email. The unlock code will be sent to you by email.

The software can also be activated by telephone by calling PTI Technical Support at (866) 213-5135. Be sure to have the Serial Number and Machine Key ready for Technical Support.

HINT
 The quickest and easiest way to activate the software is to register online.

REMEMBER
 If you email PTI, please include the site name, your name, your email address, and a phone number in case we need to contact you.

Chapter Terms

Activation	PTI's process of changing the software from Demonstration mode to live-use mode after the software has been paid for.
Adobe Reader	Program used to open and read .pdf documents.
CD	Compact Disc. Device used to store data and programs for computers.
D:\	The D drive on a computer. Usually this is the CD or DVD drive, but occasionally, the computer is setup with a different letter of the alphabet designating the CD or DVD drive.
Demonstration Mode	Feature of StorLogix that allows the program to be run for 30 days prior to purchase to allow the client time to become familiar with the product and test the functions.
Desktop	The main screen of Microsoft Windows where the icons and start bar are found.
Easy Link	Program used to interface StorLogix to various Management Software programs.
EULA	End User License Agreement. The list of rights and responsibilities of a software purchaser in agreement with the software seller.
Icon	A small picture that represents a program. Generally, clicking on the icon with the mouse will open the program represented.
Install	To load the software onto the computer.
Installation Folder	The folder on the computer where the files are kept that are required to run a program.
Load	Another name for installing software.
LogixServer	The program that controls communication between the StorLogix Software and Falcon XT.
Management Software	Software program used to manage a site. In self storage, these programs are used to rent units, send letters, assess fees, sell merchandise, and track the collections and auction process.
MSDE	Microsoft SQL Server Desktop Engine is the database engine used by StorLogix.
.pdf	Document type created by Adobe Acrobat that allows documents to be shared and read without being changed.
Register	During the licensing and activation process, this lets PTI know the purchaser of the software.
Run Command	A command on the Start menu that allows programs to be run directly by typing in the correct destination folder and program name without using an icon.
Start Bar	The bar that is usually along the bottom of a Windows Desktop showing what programs are open. Also referred to as the Taskbar.
Start Button	The button usually at the bottom left corner of a Windows Desktop on the Start Bar that access many of the programs and functions on the computer.
Wizard	A utility that allows a program or process to be completed by going through a logical series of steps in order.

CHAPTER 3: GENERAL SETUP

- **INITIAL DATABASE SETUP**
- **INITIAL STORLOGIX SETUP**
- **SETUP LOGIX SERVER**
- **LOGGING IN TO STORLOGIX**
- **NAVIGATION IN STORLOGIX**
- **SETUP PREFERENCES**
- **SETUP SCREEN**
- **SETUP COMPANY INFO**
- **SETUP SECURITY LEVELS**
- **SETUP TIME SCHEDULES**

Almost all setup of the StorLogix program is done in the Setup menu on the toolbar. The pre-installation worksheet in Chapter 1 can be completed in advance to help make the setup process easier. Refer to the glossary in the appendix of this manual for explanation of fields and terms.



Initial Database Setup

Immediately after Licensing the software, the StorLogix Select Database Server screen appears. If StorLogix is only on the local computer, select Local from the drop down menu. If StorLogix is part of a network and the actual database is on a different computer, select that computer from the drop down menu. Then click on the **Test Connection** button.

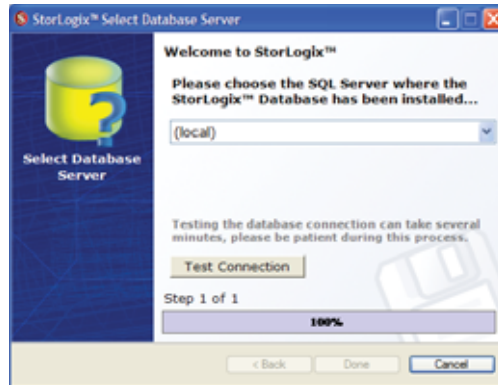


Figure 3-01: Select Database Server wizard Step 1 of 1.

APPLICATION

In most cases, StorLogix will be on the 'Local' computer, the only computer in use for the StorLogix system. In some cases though, a company may have multiple sites and will run the StorLogix database from a home office via a network. In this case, the network must already be setup and working with the StorLogix database setup on the server prior to setting up StorLogix at the site.

When the system locates a valid database, a message will appear in the middle of the window. If it cannot find the database, verify that the correct computer is selected from the drop down menu and test the connection again.

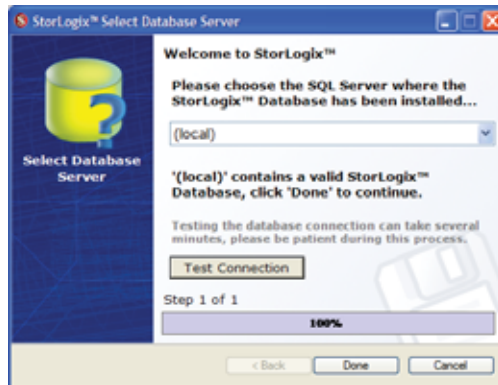


Figure 3-02: Connection Test

When a valid database is located, click on the **Done** button.

A dialog box will appear and ask if you want to connect to the database. Click on the **Yes** button to continue.

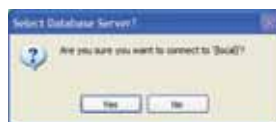


Figure 3-03: Connect to Database confirmation dialog box.



Initial StorLogix Setup

After the Database is selected, the Setup StorLogix wizard will appear. This wizard sets up the initial company information and system administrator.

Complete the information on the New Company Data screen. After completing the first New Company Data screen, click the **Next** button.

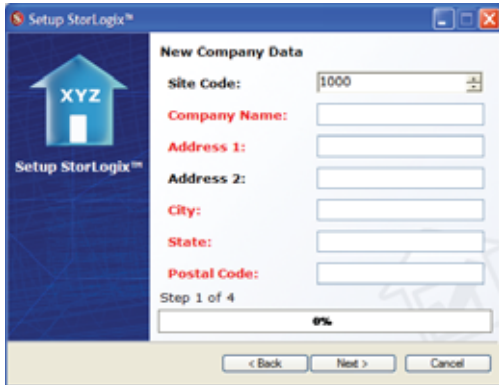


Figure 3-04: Setup StorLogix wizard Step 1 of 4 - New Company Data

Complete the second New Company Data screen. When this screen is completed, click on the **Next** button.

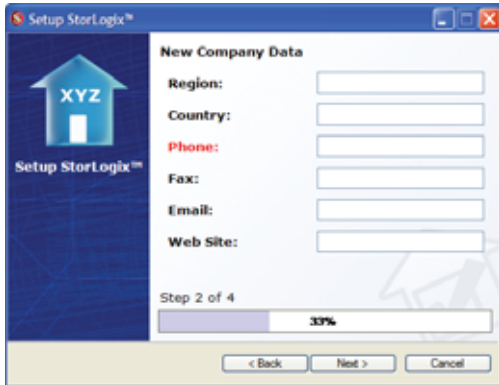


Figure 3-05: Setup StorLogix wizard Step 2 of 4 - New Company Data

Complete the Installer Information screen. Click **Next** to continue.

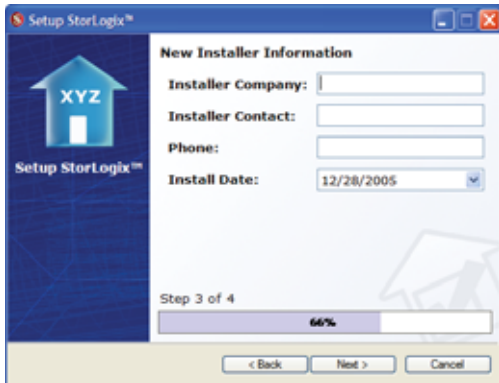


Figure 3-06: Setup StorLogix wizard Step 3 of 4 - Installer Information

????????? HINT

Fields with Red Letters must be filled out before continuing. Information entered into these fields will appear on reports and throughout StorLogix, so be accurate and fill in as much as possible.

????????? HINT

It is important to complete the Installer Information in Step 3 of 4 on the Setup StorLogix wizard. This helps to know who to call for maintenance, service, support and for future expansions to the system. This information is often lost over the years and it is helpful to know it can be found here. Always complete this screen.

Create a New Site Administrator. This person will have complete access to the system for setup. A second, default Administrator login is also created at the same time with the Login Name “Administrator” and a password “admin”. Both of these can be changed at a later date.

Click **Done** when finished.



Figure 3-07: Setup StorLogix wizard Step 4 of 4 - New Site Administrator

CAUTION

The Administrator password can be changed, but don't lose it. Any operator can be removed except the Administrator, however, if that password is lost, it cannot be retrieved.

A dialog box will appear. Click **Yes** to add the company data.

A dialog box will appear to confirm that the company data was successfully added. Click **OK** to continue.

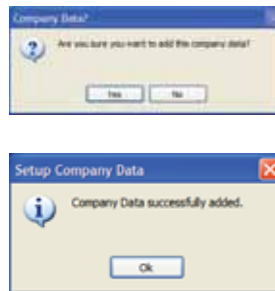


Figure 3-08: Setup StorLogix wizard confirmation dialog boxes.

HINT

All of the information in the Setup StorLogix wizard can be changed or updated at any time in the Setup Screen, Company Info and Operators sections. These are covered in Chapter 3 and Chapter 6 of this manual.



Setup LogixServer

The LogixServer Setup wizard will now appear. Confirm the Database selection in the dropdown menu and click on **Test Connection**.

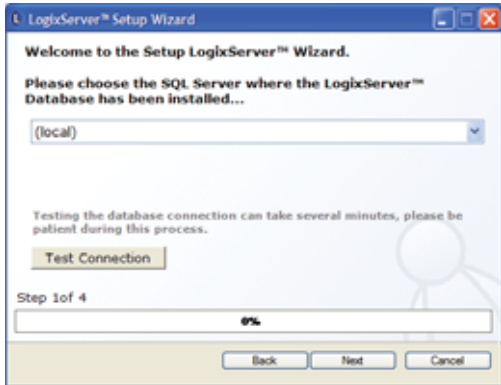


Figure 3-09: LogixServer Setup Wizard Step 1 of 4 - choosing the database connection.

When the system locates a valid database, a message will appear in the middle of the window. If it cannot find the database, verify that the correct computer is selected from the drop down menu and retest the connection. When a valid database is located, click the **Next** button.

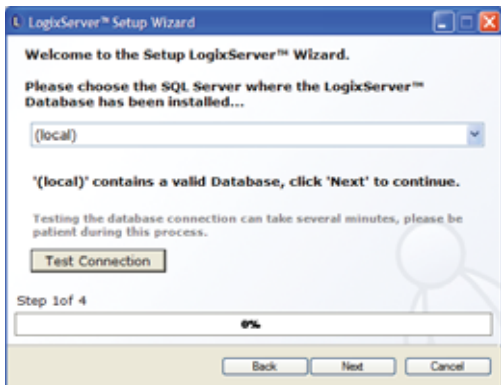


Figure 3-10: LogixServer Setup Wizard Step 1 of 4 - testing the database connection.

Select the site name that LogixServer is connected to from the dropdown menu. Click **Next** to continue.

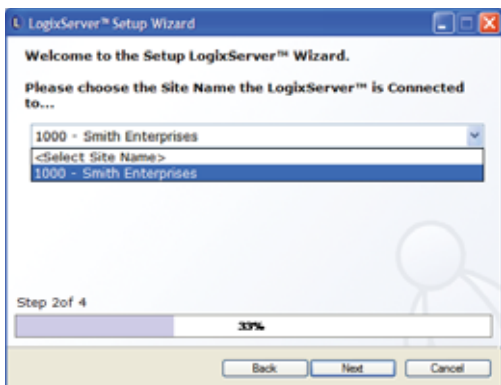
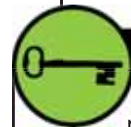


Figure 3-11: LogixServer Setup Wizard Step 2 of 4 - selecting the site name that the LogixServer is connected to.



APPLICATION

In most cases, LogixServer will be on the 'Local' computer, the only computer in use for the StorLogix system. In some cases though, a company may have multiple sites and will run the StorLogix and LogixServer databases from a home office via a network. In this case, the network must already be setup and working with the StorLogix and LogixServer databases setup on the server prior to setting up StorLogix at the site.



????????? HINT

In most cases, the site name will be the same site that was just created in the StorLogix Setup wizard. However, in some network and multi-site situations, other sites may be in the list and need to be selected.

Select the Communications Port and Baud Rate for the connection between the computer and the Falcon XT.

Click **Next** to continue.

REMEMBER

The Baud Rate for the LogixServer and the Baud Rate in the Windows Device Manager port settings must match.

Suggested Baud Rate Settings	
USB	921600
RS232	115200
Ethernet	921600

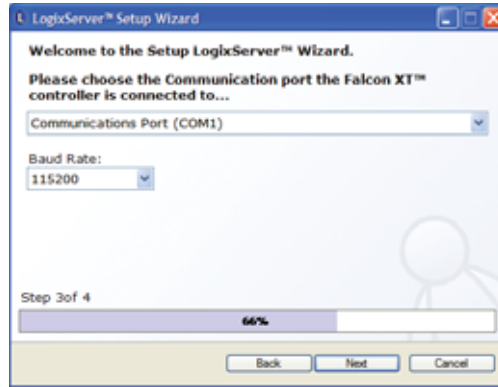


Figure 3-12: LogixServer Setup Wizard Step 3 of 4 - choosing the communications port.

Select the Time Zones for the Falcon XT and the LogixServer. In most cases they will be in the same Time Zone, but in some multi-site and network situations, they may be in different Time Zones.

Click on **Done** to complete the process.

APPLICATION

Most sites will have the LogixServer loaded on a computer that is in the same physical site as the Falcon XT that controls the access for that site. However the time zones may be different, if the company has multiple sites, each with their own Falcon XT located in different time zones and the home office has the StorLogix and LogixServer computer.

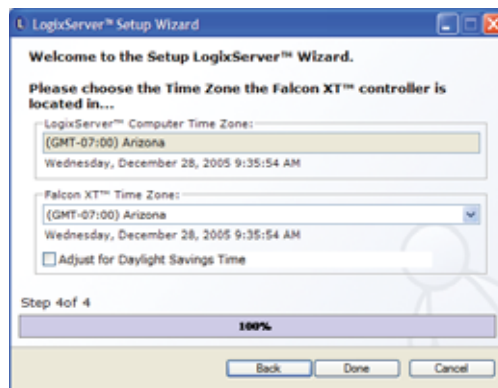


Figure 3-13: LogixServer Setup Wizard Step 4 of 4 - choosing the LogixServer and Falcon XT time zones.

A dialog box will appear. Click on the **Yes** button to save the settings. Another dialog box will then appear to confirm that the settings were successfully added. Click **OK** to continue. This will conclude the initial automatic setup screens.

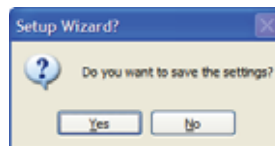
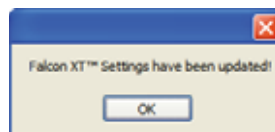


Figure 3-14: LogixServer Setup Wizard confirmation dialog boxes.





Logging In to StorLogix

The StorLogix Login screen will now appear. Type Administrator in the User Name field and Admin in the password field. Then click on the **Login** button.



Figure 3-15: StorLogix Log-In screen.

This will bring up the main StorLogix screen.



Figure 3-16: StorLogix main screen.



???????? HINT

The Administrator default login does not have to be used here. During the initial StorLogix, a second administrator should have been setup. This login could also be used.

Later, after additional Operators have been added to the system, the User Name drop down menu will contain the names of all current Operators in the system. A name can be typed in the field or selected from the drop down menu.

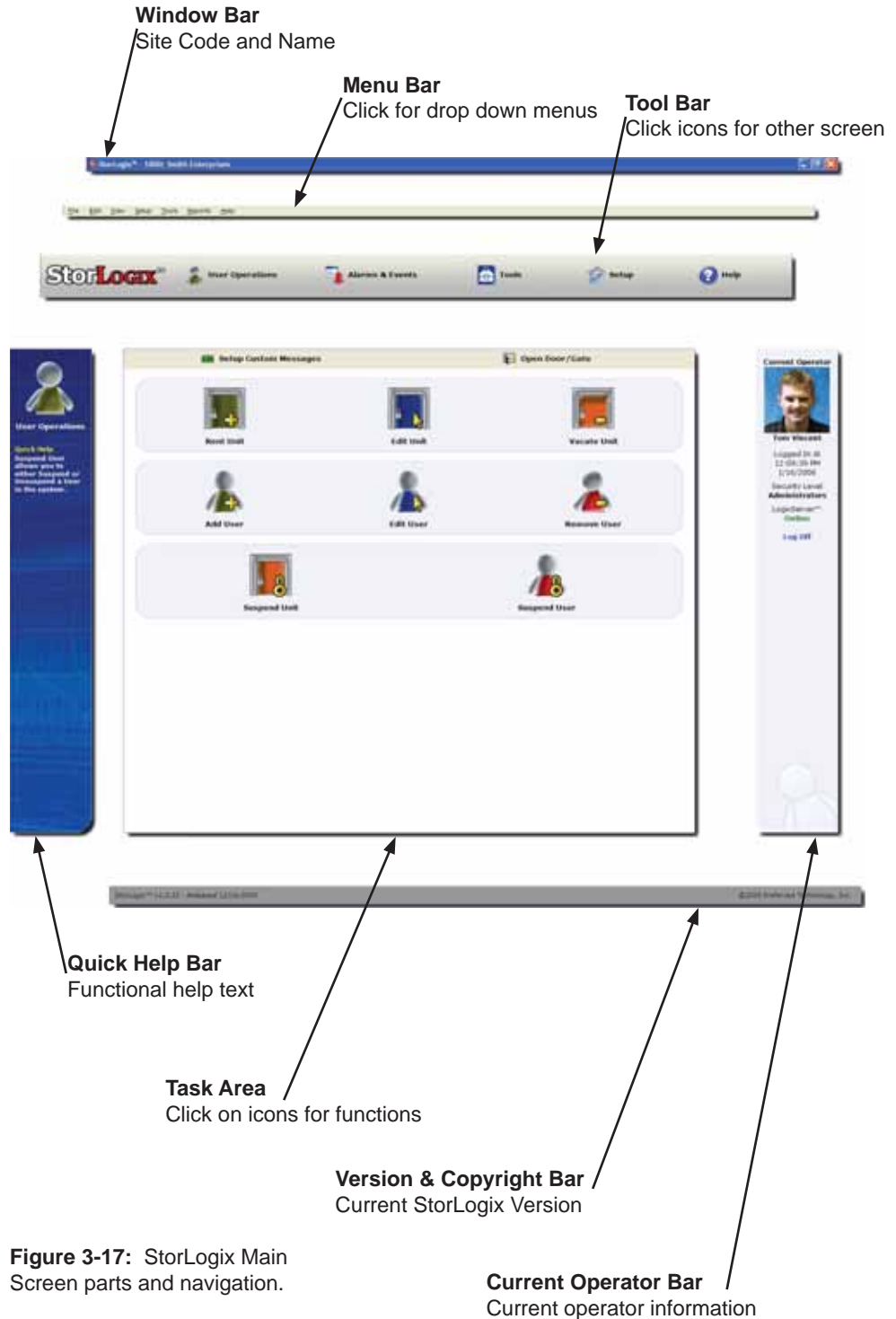
The Site drop down menu will contain the names of any sites that have been setup in the system. In most cases, there will only be the one site that has just been setup during the initial setup. However, in some multi-site situations, there will be more than one site in this field.



APPLICATION

The Change DB allows the database to be changed. This could be used in a multi-site network situation to allow an owner in a home office to log in to the databases at different sites to run reports and monitor activity. Each site would have to have its own StorLogix computer and Falcon XT and the home office would have to have its own StorLogix computer networked to the individual site computers.

Navigation in StorLogix



???????? HINT

Many functions in StorLogix can be accessed in more than one place. Often, there is an icon in the task area as well as in the menu bar. Many functions also have hot keys. These are listed in the appendix.

Figure 3-17: StorLogix Main Screen parts and navigation.

Setup Preferences

On the Main StorLogix Screen, select **Preferences** from the **Edit** menu on the menu bar to bring up the StorLogix Preferences window.

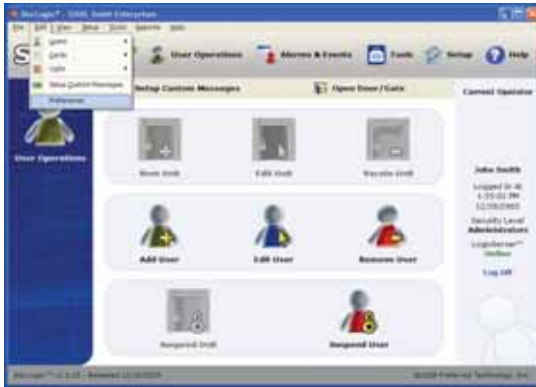


Figure 3-18: Setup Preferences

Advance Options Always On: Check this to automatically show advanced options in the Setup wizards.

Play Event Sounds: Check this to play sounds on the computer as events happen, such as sirens for alarms. Uncheck this to turn the sounds off.

Automatically Check for Updates: Set this to the frequency of minutes that StorLogix should check the internet for updates.

Check for Updates on Startup: Check this box to automatically check for updates every time StorLogix starts up.

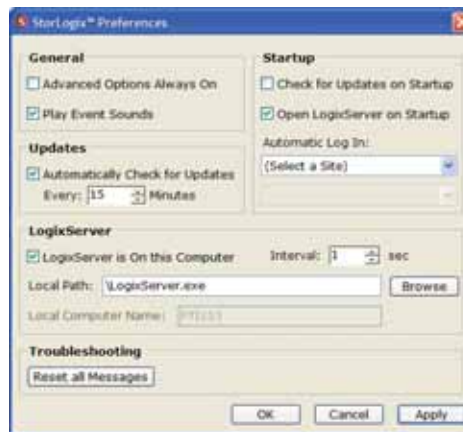
Open LogixServer on Startup: This should always be checked.

Automatic Log In: Select a site for automatic log in.

LogixServer is On this Computer: Check this box if LogixServer is on this computer. In some multi-site and network situations, LogixServer may be on a different computer. If it is on the computer, then the interval should be set to 1 second.

Troubleshooting - Reset All

Messages: There are several dialog boxes within StorLogix that allow you to select 'Do Not Show Again'. Clicking on Reset All Messages, resets this function and begins showing these dialog boxes again.



APPLICATION

Preferences do not need to be set as the default settings will serve for most sites. However, It is a good idea to review the preferences prior to continuing with the setup.

HINT

Leave advanced options turned off for basic setups. Many of these options are only for large sites with complicated controls. If an advanced option is needed, the advanced button can still be selected in the wizard.

CAUTION

If Automatic Login is selected, and the automatic login selected is an administrator, then anyone using StorLogix will have full access to the system. Also, if multiple users are logging in, it becomes impossible to tell which one made changes or to follow the audit trail.

REMEMBER

LogixServer will generally be on the same computer as StorLogix, except in some multi-site situations. If it is on another computer, then set the interval for 15 - 60 seconds depending on network performance and browse to change the path to LogixServer if necessary.



Setup Screen

From the Main Screen in StorLogix, click on the **Setup** button on the tool bar. This links to the Setup screen where most of the site setup occurs in StorLogix.



Figure 3-19: Main Screen - Click Setup on the Tool Bar

Click on each of the sections in this screen to set up the items necessary to operate the site.

PLEASE NOTE: The Setup Screen is arranged in order and should be completed in this order. Some items that are further down the list are dependent on the completion of previous items. It is best to begin with item number 1 and complete each wizard on the list in order.



Figure 3-20: Setup Screen

???????? HINT

The Main Setup screen is arranged in order of importance. Click on each of the sections in order to setup the site in the easiest and most logical manner. Items in Red have not been setup yet and do not have default settings. If the site is using these functions, they must be setup prior to operating the site.



Setup Company Info

Company Info is the general information about the site that appears on reports and throughout StorLogix.

Go to the Setup Screen in StorLogix. For more information on the Setup Screen, refer to the Setup Screen section in this chapter. Click on **1. Company Info**



Figure 3-20: Setup Screen - Select 1. Company Info.

The Company Info setup wizard will appear. Click on **Add a New Company** or **Edit Current Company Data**. Click **Next** to continue.

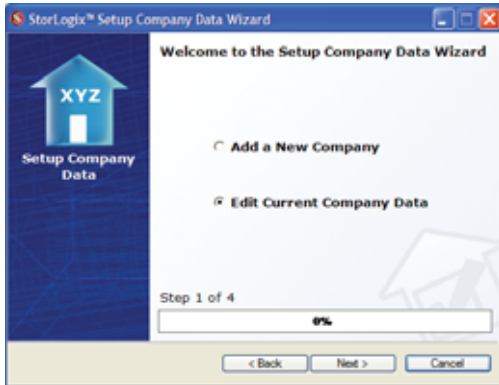


Figure 3-21: Setup Company Data Wizard Step 1 of 4 - Select Add a New Company or Edit Current Company.

Enter or change any information, then click **Next** to continue.



Figure 3-22: Setup Company Data Wizard Step 2 of 4 - Enter or change any information as necessary on this screen. Items in Red are required.

???????? HINT

Company Info was already setup during the Initial StorLogix Setup previously in this chapter. The information can be reviewed here. If everything is correct, this step can be skipped unless an additional site is being setup in a multi-site situation.

REMEMBER

The Site Code is a unique 4-digit identifier used to differentiate the site from others owned by the company. Once assigned for a site, it cannot be changed. For more information on this, see the Initial StorLogix Setup in this chapter.

Enter the new company data if an additional new site is being setup. Review and correct any information if editing existing company data. Click **Next** to continue.



Figure 3-23: Setup Company Data Wizard Step 3 of 4 - Enter or change any information as necessary on this screen. Items in Red are required.

Enter the installer information if an additional new site is being setup. Review and correct any installer information if editing existing company data. Click **Done** to complete the Company Info wizard.

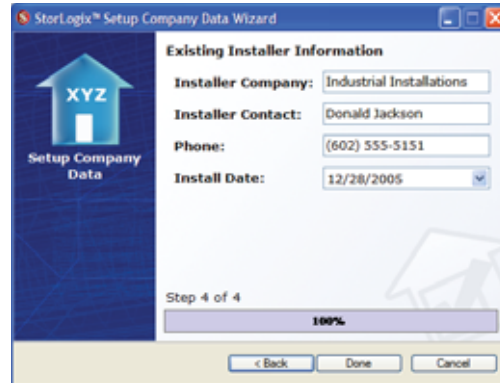


Figure 3-24: Setup Company Data Wizard Step 4 of 4 - Enter or change any installer information as necessary on this screen.

A dialog box will appear. Click on the **Yes** button to save the company data. Another dialog box will then appear to confirm that the company data was successfully added. Click **OK** to continue.

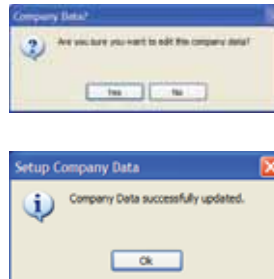


Figure 3-25: Setup Company Data Wizard confirmation dialog boxes.

REMEMBER

Region is an optional identifier used in multi-site situations such as (Southwest, Pacific, Asian, etc).

Also, remember that it is important to include installer information for future reference.

For more information on these items, refer to Initial StorLogix Setup earlier in this chapter.

Setup Security Levels



Security Levels are the permissions and privileges that operators receive for accessing StorLogix software.

Go to the Setup Screen in StorLogix. For more information on the Setup Screen, refer to the Setup Screen section in this chapter. Click on **2. Security Levels**.



Figure 3-26: Setup Screen - Select 2. Security Levels.

The Security Levels setup wizard will appear. Click on **Add**, or select a Security Level and click on **Edit** or **Remove**. Click **Next** to continue.

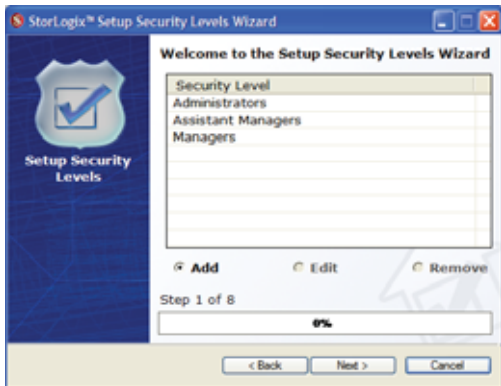


Figure 3-27: Setup Security Levels Wizard Step 1 of 8 - To Add an additional security level, click on Add a New Company. Click on a site in the list and then Edit or Remove to make changes or remove the site.

Enter or change the Security Level description and review the File Menu options list for authorized access. Click **Next** to continue.



Figure 3-28: Setup Security Levels Wizard Step 2 of 8 - Review the File Menu options to check any that operators in this security level should have access to or uncheck any that they should not have access to.

APPLICATION

There are three default security levels already setup. It is a good idea to choose edit and review each of these security levels to customize them to the site. Generally, however, Administrators should have access to every part of the software.

CAUTION

Do Not remove the Administrator Security Level or there may be no way to access or change parts of the system at a later date, especially if those have been blocked from other security levels.

HINT

Having different security levels for Owners, Managers, and Employees helps to keep individuals out of areas of the software where they do not belong and helps prevent unauthorized persons from making unwanted changes to the system that could defeat the security.

APPLICATION

Change Database Connection, Import/Export, and Clear Controller Database are examples of functions that it might be a good idea to reserve for Administrators only. Edit the other Security Levels and uncheck these to block access.

Review the Edit/User Operations Menu options list for authorized access. Click **Next** to continue.

APPLICATION

Remove User, Setup User Groups, Setup Cards, and Setup Custom Messages are functions that a site might limit to Managers and Administrators.

Edit the other Security Levels and uncheck these to block access.

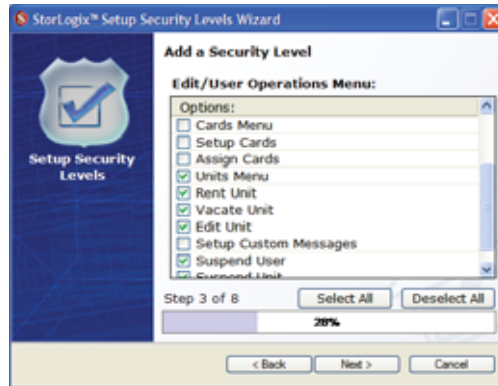


Figure 3-29: Setup Security Levels Wizard Step 3 of 8 - Review the Edit/User Operations Menu options to check any that operators in this security level should have access to or uncheck any that they should not have access to.

Review the View/Alarms & Events Menu options list for authorized access. Click **Next** to continue.

APPLICATION

Setup Alerts is a function that a site might limit to Managers and Administrators.

Edit the other Security Levels and uncheck this to block access.

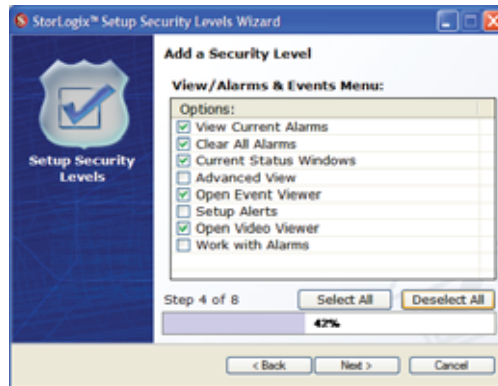


Figure 3-30: Setup Security Levels Wizard Step 4 of 8 - Review the View/Alarms Menu options to check any that operators in this security level should have access to or uncheck any that they should not have access to.

Review the Setup Menu options list for authorized access. Click **Next** to continue.

APPLICATION

The entire setup menu should probably be reserved for Administrators at a site as an unauthorized person could cause many problems by accessing and changing these.

Edit the other Security Levels and uncheck these to block access.

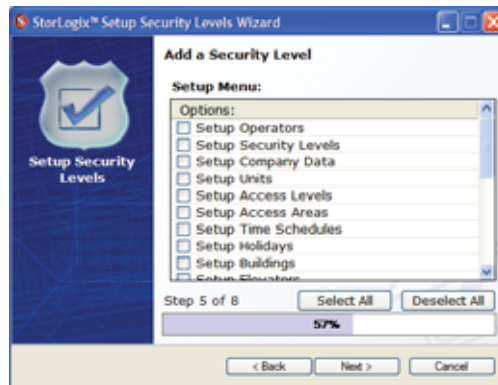


Figure 3-31: Setup Security Levels Wizard Step 5 of 8 - Review the Setup Menu options to check any that operators in this security level should have access to or uncheck any that they should not have access to.

HINT

The Select All and Deselect All buttons can make it easier to remove or add a large number of access authorizations at once.

Review the Tools Menu options list for authorized access. Click **Next** to continue.

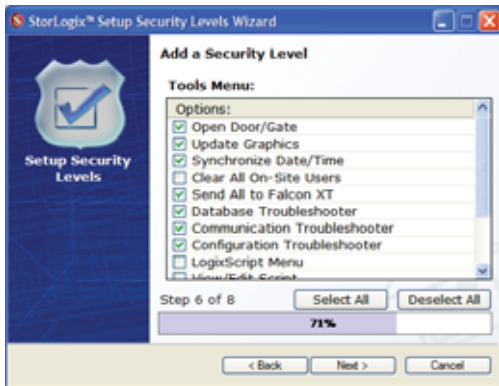


Figure 3-32: Setup Security Levels Wizard Step 6 of 8 - Review the Tools Menu options to check any that operators in this security level should have access to or uncheck any that they should not have access to.

APPLICATION

LogixScript, View/Edit Script, Download Script, Upload Script, and Run/Stop Script are functions that a site might limit to Managers or Administrators.

Edit the other Security Levels and uncheck these to block access.

Review the Options Menu list for authorized access. Click **Next** to continue.

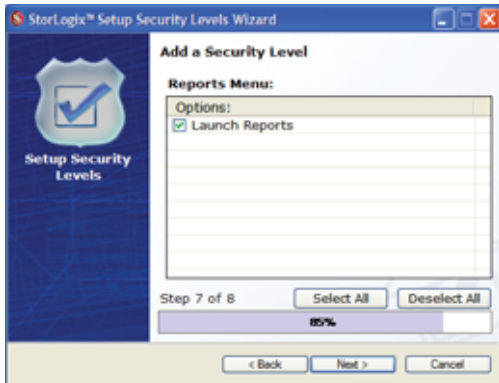


Figure 3-33: Setup Security Levels Wizard Step 7 of 8 - Review the Reports Menu options to check any that operators in this security level should have access to or uncheck any that they should not have access to.

Review the Help Menu options list. Click **Done** to complete the process.

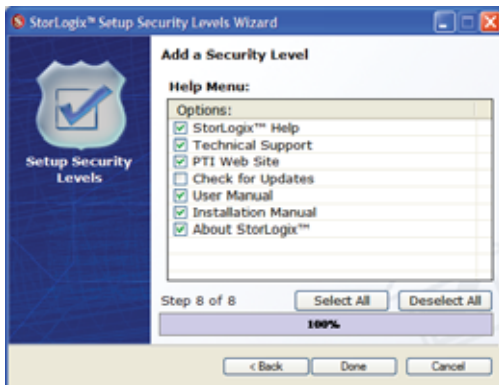


Figure 3-34: Setup Security Levels Wizard Step 8 of 8 - Review the Help Menu options to check any that operators in this security level should have access to or uncheck any that they should not have access to.

APPLICATION

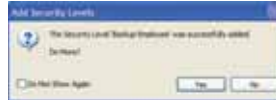
Check for Updates is a function that a site might limit to Managers and Administrators.

Edit the other Security Levels and uncheck this to block access.

A dialog box will appear. Click on the **Yes** button to save the Security Level. Another dialog box will then appear to confirm that the Security Level was successfully added. Click **Yes** to continue adding or editing security levels, click **No** to return to the Setup Screen.



Figure 3-35: Setup Security Levels Wizard confirmation dialog boxes



REMEMBER

When a StorLogix Operator is logged into the program, everything that they do is recorded in the event log for audit trail. The Administrator needs to keep this in mind if unsure whether to give them access to an area. If it is an area that they might need to use, you may want to give them access, because you can always go back and find out who made a change.

It is really easy to go overboard with security levels, locking users out of everything. The only problem with this is that they must then call an administrator every time they need to use that function. This can get quite tedious for both the employee and the administrator and can affect customer service for the company. Often, proper training is more beneficial than just locking employees completely out of areas that they will need to use on a regular basis.



Setup Time Schedules

Time Schedules are preset timetables used for access permission and scheduled functions in StorLogix.

Go to the Setup Screen in StorLogix. For more information on the Setup Screen, refer to the Setup Screen section in this chapter. Click on **3. Time Schedules**.



Figure 3-36: Setup Screen - Select 3. Setup Time Schedules.

The Time Schedules setup wizard will appear. Click on **Add**, or select a Time Schedule and click on **Edit** or **Remove**. Click **Next** to continue.

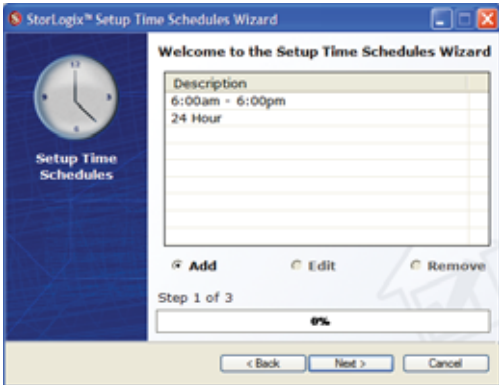


Figure 3-37: Setup Time Schedules Wizard Step 1 of 3 - Select Add to create a new time schedule or select an Existing Time Schedule from the list and click Edit or Remove.

Enter or change the Time Schedule description. Then, click **Next**.

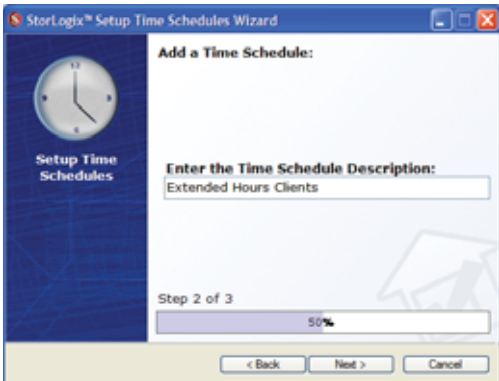


Figure 3-38: Setup Time Schedules Wizard Step 2 of 3 - Enter or change the Time Schedule Description. This should be descriptive to help select the correct one as users are entered later.

APPLICATION

There are two default Time Schedules already setup. It is a good idea to choose edit and review each of these to customize them to the site.

Time Schedules are completely customizable to the site's needs. Different ones can be set up for Managers, day shift, night shift, regular customers, extended hours customers, customers in certain buildings, etc.

HINT

It is a good idea to have one 24 hour access Time Schedule for owners and managers to be able to access the facility at any time. It is also a good idea to have one time schedule that represents the actual business hours of the site to restrict access to those hours for customers.

Some sites have extended hour access for some customers; this would be another time schedule.

Up to 255 time schedules can be added to a site.

Click inside the Green Bar for a day of the week when access is allowed.

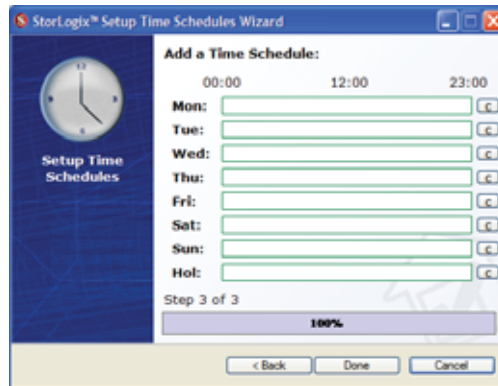


Figure 3-39: Setup Time Schedules Wizard Step 3 of 3 - Click inside the green bar for the first day of the week when access is allowed for users in this Time Schedule.

The Change Time Schedules window will appear. Set the Start Time and End Time for the first Time Span. Once the first Time Span for that day is complete, click on **Add Time Span**.

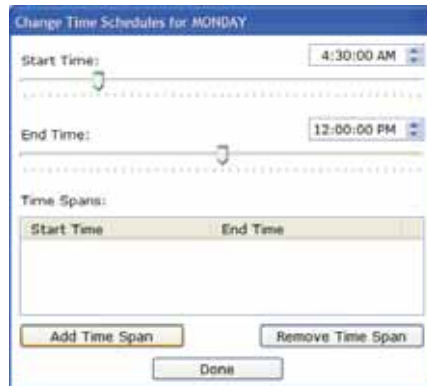


Figure 3-40: Change Time Schedules Wizard - Set the Start Time and End time one of three ways: by dragging the pull handles, by typing in the time boxes, or by using the up and down arrows by the time boxes.

Additional Time Spans can be added to the day by changing the Start Time and End Time and then clicking Add Time Span.

When all Time Spans for that day have been added, click on the **Done** button.

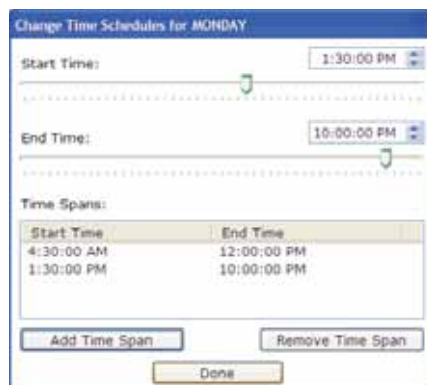


Figure 3-41: Change Time Schedules Wizard - Add additional time spans by changing the time schedule and clicking on Add Time Span. When complete, click the Done button.

APPLICATION

Time schedules can be setup in conjunction with lighting zones to control lighted signs or flood lights coming on at night and going off in the morning.

Time Schedules can be setup in conjunction with advanced functions in AI Device Properties to prevent certain keypads from being used after hours such as at a back door to help prevent after hours robberies or to require high security card + pin after hours or on certain days of the week.

HINT

Time Slots are scheduled sets of time within a Time Schedule day when access is allowed or a function will be activated. In the example shown, the first time slot is from 4:30 am till 12:00 noon and the second time slot is from 1:30 pm till 10:00 pm. That would mean that users in this Time Schedule could not get on-site from 12:00 noon till 1:30 pm (for example, if the business is closed during lunch) and from 10:00 pm through 4:30 am (during the night).

Up to 4096 time slots can be input on a site.

CAUTION

One time slot can never be inside another one. For example, it is not possible to have one time slot on a day that is from 8 am till 5 pm and then add another that is from 9 am till 4 pm on the same day. Time slots must always be in successive order with breaks of time in between.

After all time spans have been added for that day. The Time Schedules wizard will show the access hours for that day in green with white space for the time when access is denied. Often, the same time schedules are repeated for multiple days during the week. Click on the **C** button next to the completed time schedule day to copy the time schedule to other days of the week or holidays.

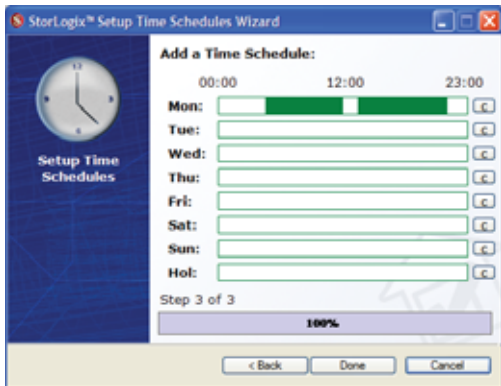


Figure 3-42: Setup Time Schedules Wizard Step 3 of 3 - Copying the Time Slots to other days of the week and holidays.

Place a checkmark beside any days that will have the same time schedule. Click **Done** to continue.

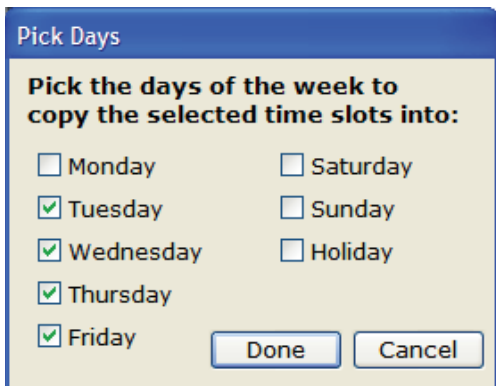


Figure 3-43: Pick Days to copy the selected time slots to.

A dialog box will appear to confirm whether to copy the time schedules to the new days. Click **Yes** to continue.

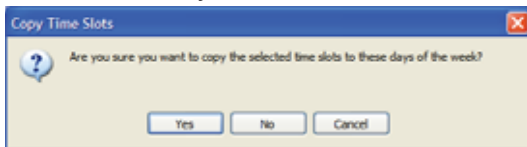


Figure 3-44: Copy Time Slots and Update Time Slots confirmation dialog boxes.



REMEMBER

Holidays can be used to set specific days during the year when business hours or access hours change, restricting access or closing it off altogether.

Holidays are only used if a site has different business hours on holidays or is closed. The actual authorized holiday hours are setup individually for each Time Schedule.

This could be used to allow employee access to a site during a holiday while preventing customer access, to close all access to the site on certain days, or to just limit the access hours on those days.

The Time Schedules wizard will now show the time schedules for each of the days of the week that were copied.

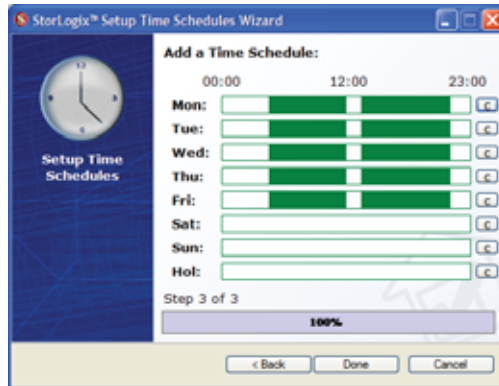


Figure 3-45: Setup Time Schedules Wizard Step 3 of 3 - Click inside the green bar for another day of the week when access is allowed for users in this Time Schedule.

To add a different time schedule for other days of the week, click inside the green box for that day and add the new time span(s) as previously done for the other day(s).

The Time Schedules wizard will now show the time schedules for each day that has been setup. Continue setting up the time schedules for each day of the week and holidays until complete. When all days are complete for this time schedule, click on the **Done** button.

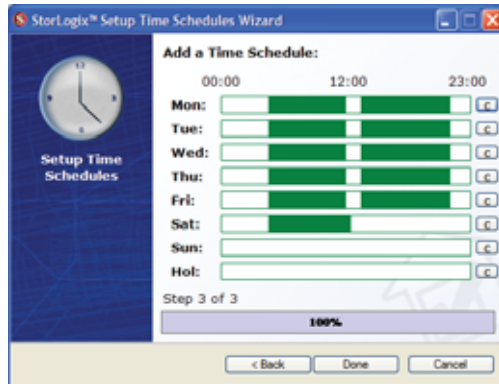


Figure 3-45: Setup Time Schedules Wizard Step 3 of 3 - Click Done when finished

A dialog box will appear. Click on the **Yes** button to save the Time Schedule. Another dialog box will then appear to confirm that the Time Schedule was successfully added. Click **Yes** to continue adding or editing Time Schedules, click **No** to return to the Setup Screen.

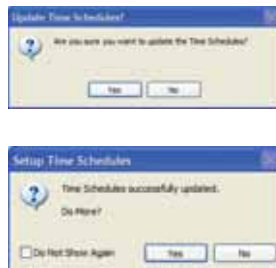


Figure 3-46: Update Time Schedules confirmation dialog boxes.

CAUTION

Be careful not to delete or remove Time Schedules that already have clients assigned to them without changing the Time Schedules for those users.

Chapter Terms

Administrator	User with full rights to setup or change any part of StorLogix.
Advanced Options	Options in the Setup Screens that offer a higher level of customization for complex site setups.
Automatic Login	This function enables a user to double-click on the StorLogix icon and automatically open StorLogix without entering a password.
Baud Rate	Communications speed between devices.
Change DB	Change database allows the database to be changed for multi-site setups.
Current Operator Bar	Area of the StorLogix main screen to the right of the Task Area that shows the current operator who is logged in, when they logged in, their security level, and the communications status with Falcon XT.
Database	A collection of information organized in such a way that the computer program can quickly access it.
Ethernet	A type of Network setup for computers to allow multiple computers to be connected together.
Event Sounds	Sounds in StorLogix that can be heard if the computer has speakers. These can alert the user to different events. StorLogix has several default sounds, however, the user can change these if desired. For example, a siren sound will occur when an alarm event happens.
Local Computer	The computer that is being used or worked on at the moment.
Login	To enter a valid user name and password so that StorLogix recognizes the user and allows them access.
LogixServer	The program that controls communication between the StorLogix Software and Falcon XT.
Menu Bar	The bar immediately below the Window bar that allows access to drop down menus that contain most of the StorLogix functions by clicking on a word.
Network	Two or more computers linked together to access shared files and programs.
Preferences	System-wide user settings that can be customized for the site.
Quick Help Bar	Bar on the left side of the task bar that contains help text giving some explanation of the icon that the cursor is floating over.
Red Letter Fields	These are required fields in StorLogix.
Region	An optional field in StorLogix to identify the site when a single company owns multiple sites. (i.e. Southwest, Pacific, Asian, etc).
Security Level	Security Levels are the permissions and privileges that operators receive for accessing StorLogix software.
Setup Screen	The screen in StorLogix where almost all of the setup for StorLogix and Falcon XT occurs.
Site Code	An optional four digit identifier that can be used to identify individual sites when a company owns multiple sites. Many companies have store numbers that this could be used for.
Task Area	The central part of the StorLogix screen where the Icons are found.

Time Schedules	Preset timetables used for access permission and scheduled functions in StorLogix.
Time Slots	Individual spans of time within a time schedule.
Time Zone	In StorLogix, this refers to the 24 zones of the earth used for setting clocks. In previous Falcon systems, this referred to a function that was similar to a combination of Time Schedules and Access Areas.
Tool Bar	The bar immediately beneath the menu bar that contains the five main functions of StorLogix.
Updates	A new version of software that contains improvements, new features, fixes, and other relevant changes.
USB	Universal Serial Bus. A communications protocol. One of the three ways that the Falcon XT can be connected to the StorLogix computer.
Version & Copyright Bar	The bar along the bottom of StorLogix that shows the current version and copyright information.
Window Bar	The Bar along the very top of the StorLogix screen that shows the Site Code and Site Name as well as having the maximize/minimize and close icons.

CHAPTER 4: DEVICE SETUP

- **ENROLL AI DEVICES**
- **SETUP RELAYS**
- **SETUP RELAYS - ADVANCED**
- **VIRTUAL RELAYS**
- **SETUP INPUTS**
- **SETUP INPUTS - ADVANCED**

The AI Devices, Relays, and Inputs all need to be setup so that they will function with StorLogix. These devices can be setup individually, however, it is much easier to have them installed, connected to the Falcon XT, with the Falcon XT connected to the StorLogix Computer. If this is already done, then setup is easy, because StorLogix automatically takes care of some of the process.



Enroll AI Devices

Enroll AI Devices is used to define the AI Devices connected to the Falcon XT. AI Devices include keypads, multiplexers, relay boards, and wiegand devices.

Go to the Setup Screen in StorLogix. For more information on the Setup Screen, refer to the Setup Screen section in Chapter 3. Click on **4. Enroll AI Devices**.



Figure 4-1: Setup Screen - Select 4. Enroll AI Devices.

The Enroll AI Devices wizard will appear. AI Devices that are connected to the system, but not yet defined will be highlighted in red.

Select the first AI Device from the list and then click on **Edit**.

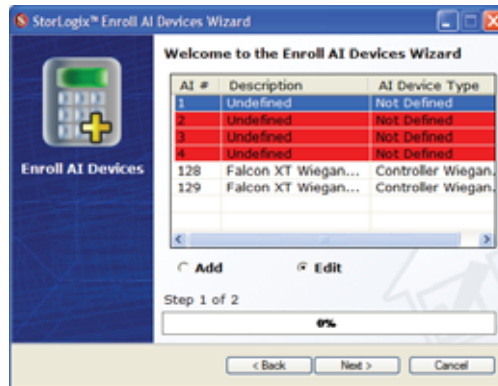


Figure 4-2: Enroll AI Devices Wizard Step 1 of 2 - Select an AI Device from the list. Click on Edit and then Next to continue.

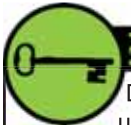
Click **Next** to continue.



REMEMBER

Be sure that all AI Devices are connected to the Falcon XT and the Falcon XT is connected to the StorLogix before performing this step.

Also, make sure that each remote AI Device is addressed with no duplicate addresses.



HINT

Devices can be added using the Add function if they were not already connected to the system, however, it is much easier to perform this process if all devices are already connected and addressed.

Select the AI Device type from the drop down list, then enter a description for the AI Device such as Front Gate Entry Keypad, Front Gate Exit Keypad, Balcony Door Keypad, or Building A West End Multiplexer. Be descriptive to make event locations easier to recognize later. Click **Done** to complete the process.

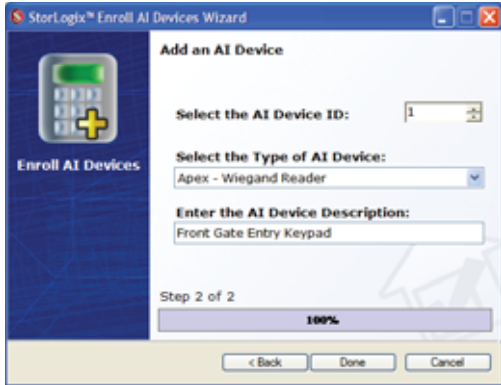



Figure 4-3: Enroll AI Devices Wizard Step 2 of 2 - If Adding the AI Device, the AI Device ID can be changed to match the AI Device. If editing an existing device that was located by StorLogix, this number cannot be changed.



APPLICATION

If the pre-installation worksheet in Chapter 1 was completed, then it should be easy to see where each AI Device is on the site, what the AI Device ID is, what type of device it is, and what purpose it serves.

A dialog box will appear. Click on the **Yes** button to save the AI Device. Another dialog box will then appear to confirm that the AI Device was successfully edited. Click **Yes** to continue editing AI Devices, click **No** to return to the Setup Screen.



Figure 4-4: Enroll AI Devices confirmation dialog boxes.

Continue the process until all AI Devices are enrolled. When complete, there should be no red highlights in Step 1 and each device should have a Description and AI Device Type.

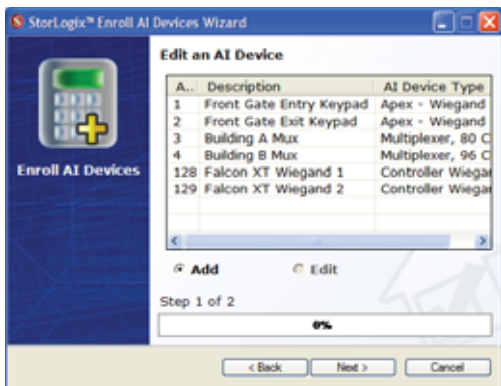


Figure 4-5: All devices enrolled. There should be no devices highlighted in red and all devices should show a type and description.

Setup Relays

Relays are the switches that control functions on the site, such as opening gates, unlocking electronic door strikes, turning on lights, activating elevator floor buttons, and sounding sirens.

Go to the Setup Screen in StorLogix. For more information on the Setup Screen, refer to the Setup Screen section in Chapter 3. Click on **5. Relays**.



Figure 4-6: Setup Screen - Select 5. Relays

If the AI Devices were setup under Enroll AI Devices, then the standard relays for each AI Device will already be in the dropdown list. Select a relay from the list and click on **Edit**. Click **Next** to continue.

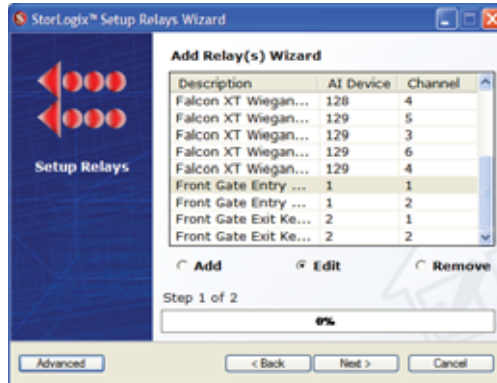


Figure 4-7: Setup Relays Wizard Step 1 of 2 - Select a Relay from the list. Click on Edit and then Next to continue.



Relays can be added using the Add function, however, generally they are already listed when AI Devices are setup in the Enroll AI Devices function shown previously in this chapter.

Adding relays from scratch is usually only done when adding Virtual Relays for LogixScript as shown in the Advanced Relay function in this chapter and the LogixScript function in Chapter 10.

The description for the relay should already be listed as it is based on information entered in the Enroll AI Devices process. Select an activate time. Click **Done** to finish the process.

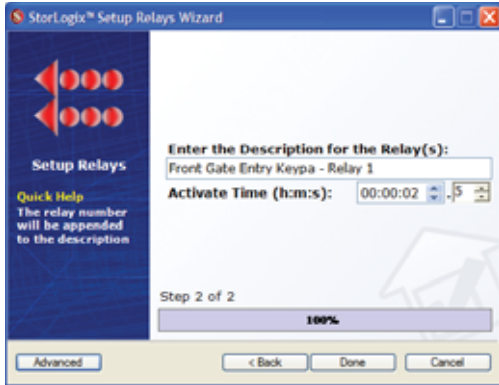


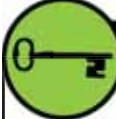
Figure 4-8: Setup Relays Wizard Step 2 of 2 - Select an Activate Time for the relay.

A dialog box will appear. Click on the **Yes** button to save the Relay.

Another dialog box will then appear to confirm that the Relay was successfully edited. Click **Yes** to continue editing relays, click **No** to return to the Setup Screen.



Figure 4-9: Setup Relays Wizard confirmation dialog boxes.



??????? HINT

The Activate Time is the time that the relay should hold for when activated. The first field has hours:minutes:seconds. The second field is tenths of a second.

2 - 3 seconds is a suggested relay time for many types of gates. 5 - 10 seconds or more is suggested for most electronic doors. Other devices such as sirens and alarm shunts may need to be held for longer times.

Setup Relays - Advanced

Relays have advanced features that can be setup.

If the StorLogix Preferences were setup with 'Advanced Menus Always On', then the advanced steps will already be visible. If not, from Step 2 of the relay setup process, click on the **Advanced** button at the bottom left corner of the field. This adds an advanced Step 3. Click the Next button from Step 2 to get to this Advanced screen.

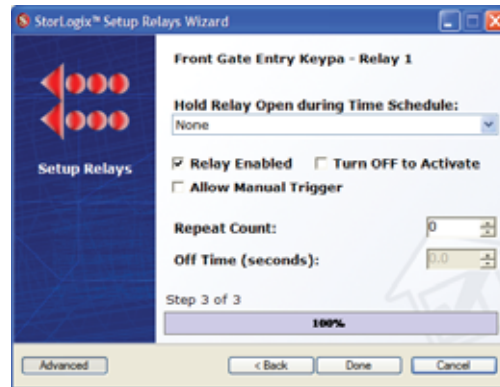


Figure 4-10: Setup Relays Wizard Advanced Step 3 of 3 - Select the desired advanced functions and click on Done.

In this screen, the relay can be programmed with additional advanced features:

Hold Relay Open During Time Schedule: Select a time schedule from the list and StorLogix will trigger the relay and hold it open during those hours.

Relay Enabled: Check this box to enable the relay. Uncheck the box to disable the relay.

Turn OFF to Activate: This box is checked only when a relay was accidentally wired backwards and needs to be made functional without rewiring the relay.

Allow Manual trigger: Check this box to allow the relay to be manually triggered from the StorLogix Tools Menu or Function Key F6.

Repeat Count: Set this to allow the relay to trigger on and off again several times.

Off Time (Seconds): This works with the repeat count. It is the number of seconds and tenths of seconds between each repeat that the relay is off.

APPLICATION

Hold Open During Time Schedule could be used to hold a front gate open or keep an alarm shunted during business hours.

APPLICATION

There are more advanced relay functions that can be used by adding virtual relays. These are briefly covered later in this chapter and much deeper in the LogixScript section of Chapter 10.

Virtual Relays

Virtual Relays are switch commands that are setup in StorLogix that can perform actions within the system based on their status (either on or off). There is no actual physical switch involved, only system status.

Virtual Relays can be used in conjunction with existing functions to perform various tasks or they can be used with the LogixScript to create a variety of custom tasks for the site. See LogixScript in Chapter 10.

The primary use for Virtual Relays is with the panic alarm function and the silence alarm function. In conjunction with Alarm Zones (see Chapter 5), virtual relays provide the trigger for these two functions. To set these up, make sure the advance button is on and select Add in Step 1 of 3 on the Setup Relays Wizard and click on **Next**.

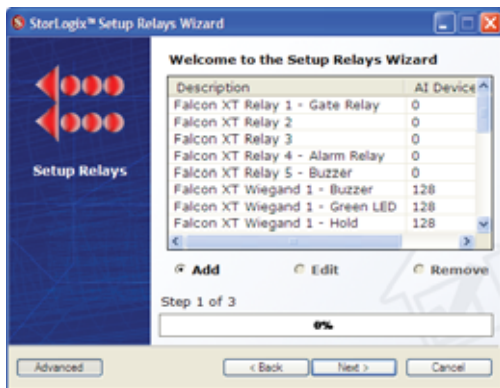


Figure 4-11: Setup Relays Wizard Advanced Step 1 of 3 - Virtual Relays. Click on Add and then click Next. Make sure that the Advanced functions are on as Virtual Relays are part of the Advanced functions.

Then select Virtual Relay. This will automatically bring up 0-Virtual Relay under the Select the AI Device. Enter a description for the relay and then select the Activate time in hours, minutes, seconds, and tenths of seconds. Click **Next** to continue. Complete Step 3 of 3 as shown in Setup Relays - Advanced on the previous page.

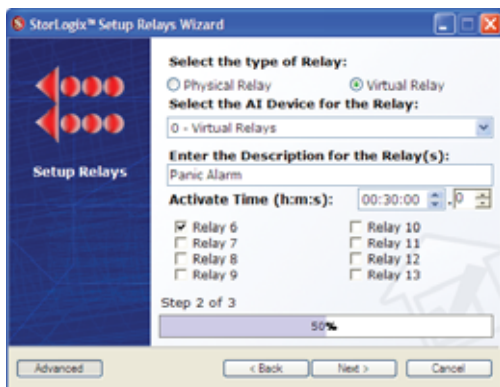


Figure 4-12: Setup Relays Wizard Advanced Step 2 of 3 - Virtual Relays.

HINT

Virtual Relays are generally used with LogixScript for creating advanced custom functions as solutions to specific site needs. Virtual Relays are always setup in other functions such as Alarm Zones or LogixScript, but they must be created and named here first.

APPLICATION

The Panic Alarm function allows the employee to wear a pendant or have a button under the desk that triggers an audible or silent alarm in a panic situation such as a robbery or assault.

The Silence Alarm function allows the manager to wear a pendant or have remote buttons on a site that allows them to silence alarms remotely while out on the site without having to return to the StorLogix Computer in the office.

Setup Inputs

Inputs are alarm point connections for devices such as door alarm contacts, motion sensors, glass break sensors, and tamper switches.

Go to the Setup Screen in StorLogix. For more information on the Setup Screen, refer to the Setup Screen section in Chapter 3. Click on **6. Inputs**.



Figure 4-13: Setup Screen - Select 6. Inputs.

Select an input from the list and click on Edit. Then click on **Next**.

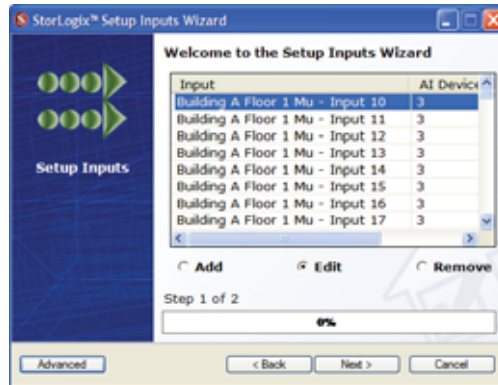


Figure 4-14 Setup Inputs Wizard Step 1 of 2 - Select an input from the list. Click on Edit and then Next to continue.

HINT
 If the AI Devices were entered under the Enroll AI Devices, then all alarm input Devices (Multiplexers, APEX Keypads, and 8-channel Relay Boards) will already have the inputs listed. StorLogix does this automatically. If all of the inputs are door contact switches and built-in tamper switches, then this wizard will not be needed. This wizard is only needed if manually entering inputs into the system or if the AI Devices were not entered under the Enroll AI Devices.

Enter a description for the Input. It is helpful to be descriptive to help with event location later (for example: Building B West Stairwell Motion).

Then, select the sensor type from the drop down list. Sensor Types are described in the Application note to the left.

Click **Done** when finished.

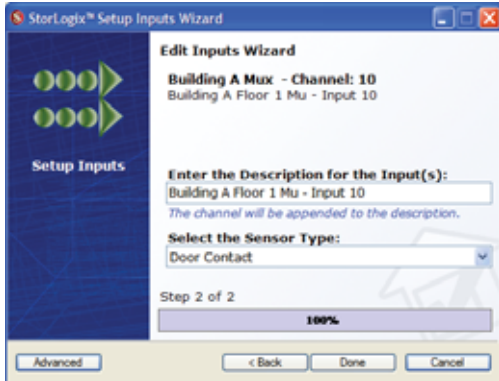


Figure 4-15 Setup Inputs Wizard Step 2 of 2 - Enter a description for the Input and select the sensor type.

A dialog box will appear. Click on the **Yes** button to save the Input.

Another dialog box will then appear to confirm that the Input was successfully updated. Click **Yes** to continue editing inputs, click **No** to return to the Setup Screen.



Figure 4-16 Setup Inputs Wizard confirmation dialog boxes.



Sensor Types:

Door Contact: This reports as a door open, door close, or door alarm.

Motion Sensor: This reports as a motion alarm if no authorized person is logged into that area. If an authorized user is logged into that area, no alarm or event is generated.

Glass Break Sensor: This always reports an alarm if triggered, whether an authorized user is logged in the area or not.

Device Tamper: These are tamper switches built into AI Devices. Unless Tamper Switches are deactivated in the AI Device programming or in StorLogix, these will always report as an alarm if the AI Device is opened.

Input Tamper: This allows the installer to place tamper switches on other devices such as motion sensors, junction boxes, security cabinets, etc. These will always report an alarm if that item is tampered with.

Setup Inputs - Advanced

Inputs have advanced features that can be setup. If the StorLogix Preferences were setup with 'Advanced Menus Always On', then the advanced steps will already be visible. If not, from Step 2 of the Input setup process, click on the **Advanced** button at the bottom left corner of the field. This adds advanced Steps 3 & 4. Click the Next button from Step 2 to get to this Advanced screen.

Select the advanced options for this input.

Sensor is Wireless: If the sensor is a PTI wireless transmitter, check this box and enter the **Transmitter ID** in the next field.

Enable Swinger Shutdown: Roll-up doors sometimes shake with traffic vibration or wind. If this becomes excessive, causing the door alarm to sound, check this box and then input a Time Period and Swinger Count in the following fields. The Time Period is the length of time that the switch must remain in the same state before the alarm sounds. This is generally set at 1 - 3 minutes. Swinger count is the number of times the switch must be in alarm state before the alarm sounds.

Sounds Alarm: If this is checked, then the door alarm will sound if triggered. If this is unchecked, then the activity will report, but the alarm will not sound.

Click **Next** to go to Step 4 of the advanced options.



Figure 4-17 Setup Inputs Wizard Advanced Step 3 of 4 - Select advanced options.

In Step 4 of 4 of the advanced options, complete the selections for the input.

Active in OPEN State: This is checked only if the door switch type is wired backward or if it is the type of switch that triggers on open instead of closed.

Report Activity: This should normally be checked. Uncheck this box only if a alarm switch is malfunctioning and giving false alarms (only until the switch is repaired).

Ignore On-Site Activity: Check this box to prevent activity from reporting while the customer whose unit it is connected to is on-site.

Click **Done** to complete the process.



Figure 4-18 Setup Inputs Wizard
Advanced Step 3 of 4 - Select
advanced options.

Chapter Terms

Activate Time	The amount of time in Hours, Minutes, Seconds, and tenths of a second that a relay will remain activated when triggered.
Active in Open State	This option is chosen when a relay has been wired backwards. It allows the relay to be used without rewiring by switching its functional state in the software.
Address	Another term for AI Device ID, especially in connection with previous Falcon systems.
AI Device ID	The unique identifier number programmed in to each AI Device to differentiate it from other AI Devices when communicating to the Falcon XT. Referred to as Address in previous Falcon Systems.
Alarm Shunt	A relay that bypasses an alarm switch device for a specific period of time. For example, the front door alarm may be shunted for 60 seconds to allow the employee to exit the site after setting the alarm without triggering the alarm. After 60 seconds, then the door alarm would be live.
Allow Manual Trigger	An option to allow a gate or door to be opened by pressing F6 on the keyboard at the StorLogix computer.
Device Tamper	Tamper switches built into AI Devices. These always report as an alarm even if authorized users are logged into the area.
Door Alarm Contact	Hard wired switches that are installed on doors to indicate if the door is open or closed.
Door Switch	Another name for Door Alarm Contacts.
Glass Break Sensor	Sensors that can detect if a window is broken by monitoring for the sound frequency of the glass breaking. Refer to Manufacturers Instructions for installation and operation of these devices. In StorLogix, these always report an alarm, even if authorized users are logged into the area.
Input Tamper	A tamper switch installed on devices other than AI Devices by an installer. These may include tampers on motion sensors, junction boxes, security cabinets, etc. In StorLogix, these always report as an alarm even if authorized users are logged into the area.
Motion Sensor	A device that monitors for motion in an area, usually by sensing infrared heat traveling across an area. In StorLogix, these only report as an alarm if there is no authorized user logged into the area. If there is an authorized user logged into the area, no alarm is reported.
Multiplexer	An AI Device used to combine multiple input signals into one output data signal. It is a connection point for door alarms that feeds the information from multiple doors back to the Falcon XT.
Off Time	The time in seconds and tenths of seconds that a relay is off between repeats. See Repeat Counts.
Output	Another name for a relay in StorLogix.
Panic Alarm	An alarm button that is setup to automatically trigger an alarm zone when pressed. This may be on a pendant worn by the site manager or placed under a desktop. This can trigger a silent or audible alarm.

Physical Relay	An actual tangible electronic relay switch. For Example: there are two relay switches located in an APEX keypad that can be used to open gates or doors. See Also Relay and Virtual Relay.
Relay	A switch located in electronics used to control another device. May be physical or virtual. See Also Physical Relay and Virtual Relay.
Relay Board	An AI Device that has multiple relays on it. Generally these are used to control elevators or lighting zones, but may also be used as additional relays on a site.
Repeat Count	The number of times that a relay will trigger after being activated. These are offset by the off time.
Silence Alarm	A function in StorLogix to turn off all alarms that have been activated. Using a virtual relay, this can be setup with an alarm input button to allow a site employee to turn off the alarms remotely by pushing a remote button or pendant button.
Swinger Shutdown	Roll-up doors sometimes shake with traffic vibration or wind due to poor installation, settling of the building over time, or broken tracks. If this becomes excessive, causing the door alarm to sound, then this function can be used to allow the system to ignore door state changes that do not last for a longer period of time.
Tamper Switch	An alarm switch that is triggered when a device is opened.
Turn OFF to Activate	This option is chosen when an input is installed backwards or the wrong type has been purchased. It allows the input to be used without rewiring by switching its functional state in the software.
Virtual Relay	Switch commands setup in StorLogix that can perform actions within the system based on their status (either on or off). There is no actual physical switch involved, only system status. Generally these are used with Alarm Zones or LogixScript.
Wiegand Device	An AI Device that communicates with Wiegand Protocol Devices such as proximity card readers, fingerprint readers, or key fobs.

CHAPTER 5: SITE SETUP

- **SETUP ALARM ZONES**
- **SETUP ALARM ZONES - ADVANCED**
- **SETUP LIGHTING AREAS**
- **SETUP LIGHTING AREAS - ADVANCED**
- **SETUP BUILDINGS**
- **SETUP ELEVATORS**

Site Setup covers the physical layout issues of the site with Buildings, Elevators, Alarm Areas, and Lighting Area controls. Much of this is applicable to larger sites with multiple access areas, multiple sirens, and advanced controls for elevators and lights. Many smaller sites with only perimeter access control will not need to do any of the setup in this section.



Setup Alarm Zones

Alarm Zones are areas of the property where sirens will sound when an alarm is activated.

Go to the Setup Screen in StorLogix. For more information on the Setup Screen, refer to the Setup Screen section in Chapter 3. Click on **7. Alarm Zones**.



Figure 5-1: Setup Screen - Select 7. Alarm Zones.

HINT

There is one default Alarm Zone called the Global Alarm Area. In an alarm situation, this will sound any auxiliary sirens attached to multiplexers, Apex relays setup as alarm outputs, or sirens connected to Falcon XT Relay 4 (default).

To add a new Alarm Zone, click on **Add** and then the **Next** button.

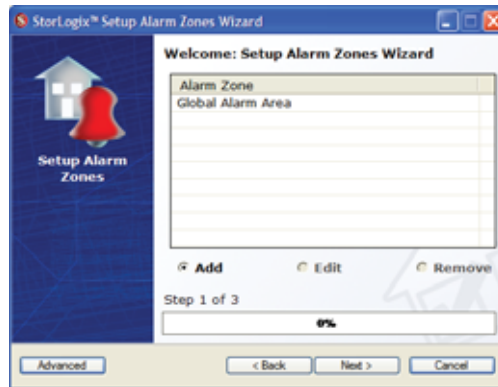


Figure 5-2 Setup Alarm Zones Wizard Step 1 of 3 - Click on Add and then Next to add a new zone. Click on a Zone in the list, select Edit and click on Next to edit an existing Zone.

APPLICATION

Start Time (Day or Night) is the beginning of the day or nighttime hours for alarms. On Time is the length of time in hours, minutes, and seconds that an alarm siren will sound if triggered within that alarm zone.

Some sites will want alarm sirens to sound longer at night than during the day. Others, especially sites near residential areas, will want alarm sirens to sound for a shorter time during the night.

Enter a name for the new alarm zone under Alarm Zone Description. Select a Start Time and an On Time for Day and Night. Click **Next**.

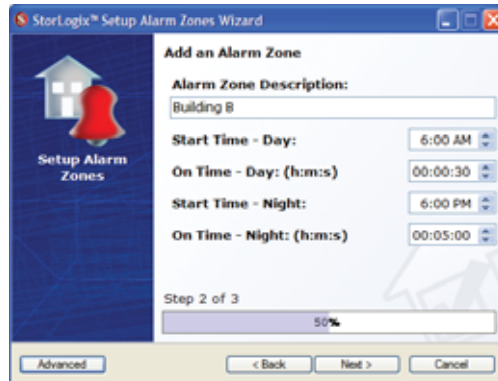


Figure 5-3 Setup Alarm Zones Wizard Step 2 of 3 - Enter or edit the Alarm Zone Description. Be descriptive so that events are reported clearly.

Select a relay to trip when the alarm is activated. This drop down list will show all of the programmable relays that exist in the system. The selected relay will need to be connected to a working siren, light, or other alarm output function. Click **Add** to add the relay to the list.

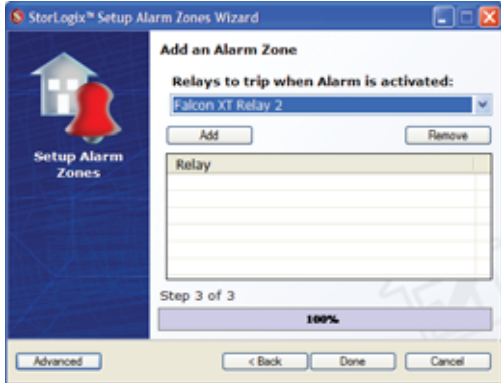


Figure 5-4 Setup Alarm Zones Wizard Step 3 of 3 - Enter or edit the Alarm Zone Description. Be descriptive so that events are reported clearly.

More than one relay can be triggered from a single alarm event. Select and add each relay for the Alarm Zone and then click **Done**.

A dialog box will appear. Click on the **Yes** button to save the Alarm Zone.

Another dialog box will then appear to confirm that the Alarm Zone was successfully edited. Click **Yes** to continue adding and editing Alarm Zones, click **No** to return to the Setup Screen.



Figure 5-5 Setup Alarm Zones Wizard confirmation dialog boxes.



REMEMBER

Physical Relays are switches that can be connected sirens, doors, gates, or lights. Alarm Zones could be used to trigger a siren and flashing light if an alarm event occurs in a given area.

Alarm Zones could also be used in conjunction with Virtual Relays and LogixScript to do things such as lockdown a door or turn on the lights if an alarm occurs in a given area.



APPLICATION

Setting up Alarm Zones in conjunction with buildings can be very useful. Sirens inside each building could be set to sound when an alarm in that building occurred.

Sirens inside a building could be set to sound longer than sirens outside the building.

Silent alarms could be setup by connecting a light relay to the Alarm Zone so that an alarm event in a given area doesn't sound a siren, but activates a light on an alarm monitoring board.

Used in connection with Alerts, the system could be set to send an email or page someone if an alarm event occurs.

Setup Alarm Zones - Advanced

Alarm Zones have advanced features that can be setup.

If the StorLogix Preferences were setup with 'Advanced Menus Always On', then the advanced steps will already be visible. If not, from Step 3 of the Alarm Zones setup process, click on the **Advanced** button at the bottom left corner of the field. This adds advanced Steps 4 & 5. Click the Next button from Step 3 to get to this Advanced screen. Click **Next** to go to the final Advanced Step.

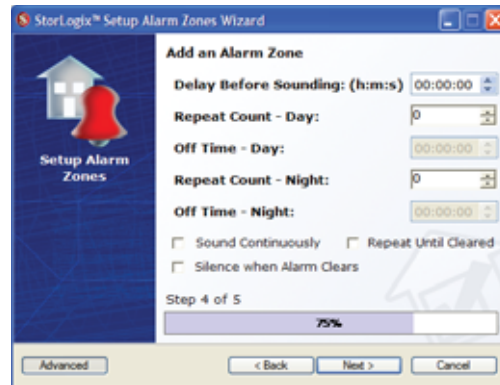


Figure 5-6 Setup Alarm Zones Wizard Advanced Options Step 4 of 5. Select the advanced options and click Next to continue. See Hint on Sidebar for more explanation of these advanced options.

Silence Relay and Panic Relay are two virtual relays that can be programmed using a wireless pendant or under desk button, so that a manager on-site can trigger the alarm to silence it or trigger a panic alarm. The panic alarm could also be used to trigger a silent alarm at a monitoring station.

Click **Done** to complete the advanced setup.

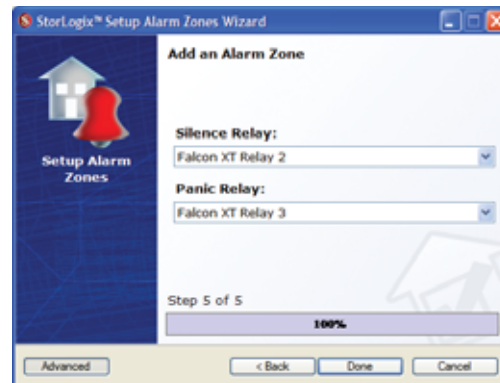


Figure 5-7 Setup Alarm Zones Wizard Advanced Options Step 5 of 5. Select the Silence Relay and Panic Relay if applicable.



Advanced Setup:

Delay before Sounding: This setting allows a delay to be set, allowing an entry alarm to be cleared before tripping an alarm panel.

Repeat Count: This is the number of times that the alarm will sound before shutting off.

Off Time: Based on the previously set On Time and the Repeat Count, this is the length of time that the alarm is off before repeating again.

Sound Continuously: If this option is checked, then the alarm will not stop sounding until a clear alarms command is entered in StorLogix.

Repeat Until Cleared: If this option is checked then the alarm will repeat based on the On Time and Off Times until cleared, ignoring the repeat count.

Silence when Alarm Clears: If this option is checked, then the alarm is automatically silenced when cleared, disregarding the silence alarm function.



Never check Sound Continuously AND uncheck Silence When Alarm Clears. This will create an alarm that can never be silenced once triggered!



Setup Lighting Areas

Lighting Areas are relays that are triggered when users in certain areas come onto the property.

Go to the Setup Screen in StorLogix. For more information on the Setup Screen, refer to the Setup Screen section in Chapter 3.

Click on **8. Lighting Areas**.



Figure 5-8 Setup Screen - Select 8. Lighting Areas.

To add a new Lighting Area, click on **Add** and then the **Next** button. If there are already Lighting Areas setup, select one from the list and click on Edit or Remove if changes are to be made.



Figure 5-9 Setup Lighting Areas Wizard Step 1 of 2 - select Add to add a new lighting area or select a lighting area from the existing list and click on edit to edit the Lighting Area and Remove to remove it. Click Next to continue.



REMEMBER

Lighting areas are most often used to save money on power bills by leaving the lights turned off for a building or area when no one is in the area and turning them on when a user with a unit in that area comes on the site. This could also be used to turn on a safety exhaust fan whenever someone enters an area that requires circulation.

Lighting Areas are really just area specific relays that can be used for many things such as climate controls based on Time Schedules to turn air conditioning or heating just before business hours and turning them down or back off after business hours to save money. They can also be used to turn on lighted signs or exterior building lights at night.



CAUTION

Do not try to setup Lighting Areas without a written plan and sketch as it can be very confusing and cost a great deal of time trying to figure out mistakes in the setup.

Enter a descriptive name for the lighting area. Then, select the relays to trigger for that lighting area. More than one relay can be selected. Select each relay and click on **Add**. When the relay(s) are selected, click on the **Done** button.

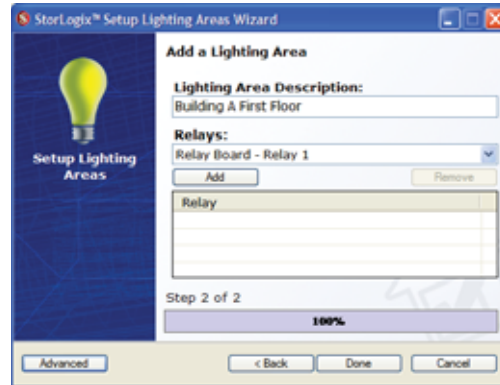


Figure 5-10 Setup Lighting Areas Wizard Step 2 of 2 - give the lighting area a descriptive name and then select the relay or relays that it will trigger.

A dialog box will appear. Click on the **Yes** button to save the Lighting Area.

Another dialog box will then appear to confirm that the Lighting Area was successfully edited. Click **Yes** to continue adding and editing Lighting Areas, click **No** to return to the Setup Screen.



Figure 5-11 Setup Lighting Areas Wizard confirmation dialog boxes.

Lighting Areas can be Added or Edited as needed by clicking on the **Add**, **Edit**, or **Remove** buttons from the first screen of the Lighting Area setup wizard.



Figure 5-12 Setup Lighting Areas Wizard Step 1 of 2 - Editing and Removing Lighting Zones.

APPLICATION

A single Lighting Area can be used to trigger multiple relays. This could be used in sites with multiple floors so that a user logging into the site at the entrance keypad would automatically turn on the lights on the floor in the building where their unit is, but also the first floor lights in the same building so that they can get to the elevator.

HINT

Lighting Areas are set up in this area of the program, but are not actually put in place until associated with units and users. Refer to Chapter 7 in this Setup Manual for information on setting up Units. Refer to the Operations manual for information on adding Users.

Setup Lighting Areas - Advanced

Lighting Areas have advanced features that can be setup.

If the StorLogix Preferences were setup with 'Advanced Menus Always On', then the advanced steps will already be visible. If not, from Step 2 of the Access Area setup process, click on the **Advanced** button at the bottom left corner of the field. This adds an advanced Step 3. Click the Next button from Step 2 to get to this Advanced screen.

Pass Through Lighting Area: This is used if a user must pass through one lighting area to get to another such as multiple hallways in a building, or a stairwell that leads to the hallway with their unit in it. This turns the lights on for that area as well as the lighting area that the user's unit is in.

On During Time Schedule: This turns the lighting area on during the time schedule selected and off after those hours. After hours, the lights only come on if a user with a unit in that area comes onto the site.

Trip on Input: This allows a lighting area to be tripped with an input such as a motion sensor or door switch being opened.

On for Time: This is associated with Trip on Input. If Trip on Input is selected, then this is the amount of time that the Lighting Area will stay on after input.

Off Delay Time: This is the length of time that the lights stay on after the last user with a unit in the area exits the site.

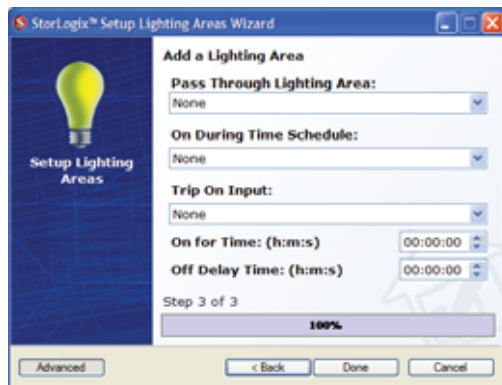


Figure 5-13 Setup Lighting Areas Wizard Advanced Options Step 3 of 3 - Select the applicable advanced options and click Done.



APPLICATION

The On During Time Schedule function could be used to control exterior lights or a lighted sign so that they come on at night and turn off in the morning. Just create a Time Schedules with the hours that the lights or sign should be on and then associate the relay to a Lighting Area and the Time Schedule in here after it is wired.

Pass Through Lighting Areas are used in situations where a user must go through more than one Lighting Area to get to their unit. For Example, a building may have one main hallway from the front door with multiple side hallways. The main hallway would be a pass through lighting area and each of the side hallways would be their own individual lighting areas. That way, when a user comes on-site, the main hallway and their hallway will be lit.



Setup Buildings

Buildings are the actual separate structures on a property that are access controlled. Buildings are setup for elevators and access areas only. If neither function is being used, then buildings do not need to be setup.

Go to the Setup Screen in StorLogix. For more information on the Setup Screen, refer to the Setup Screen section in Chapter 3. Click on **9. Buildings**.



REMEMBER

Buildings only need to be set up if they are access controlled with keypads or wiegand devices or if there are elevator inside the building that are controlled by keypad or wiegand device. If the site is not using access control keypads or wiegand devices on the structures or elevators within a site, then Building Setup does not have to be done.



Figure 5-14 Setup Screen - Select 9. Buildings.

Click on **Add** button and then **Next** to add a building to the property.

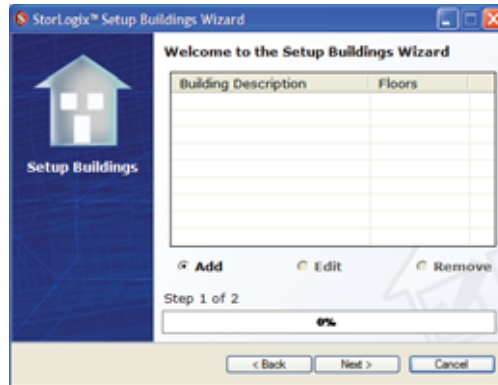


Figure 5-15 Setup Buildings Wizard Step 1 of 2 - select Add to add a new Building. Click Next to continue.

Enter a description and number of floors in the building. Click **Done**.

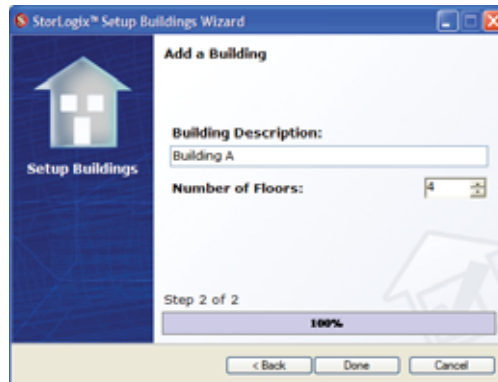


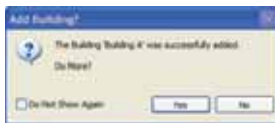
Figure 5-16 Setup Buildings Wizard Step 2 of 2 - Enter a description of the building and the number of floors. Include basement levels, ground level, as well as any levels above ground in the number of floors.

A dialog box will appear. Click on the **Yes** button to save the Building.

Another dialog box will then appear to confirm that the Building was successfully added. Click **Yes** to continue adding and editing buildings, click **No** to return to the Setup Screen.



Figure 5-17 Setup Buildings Wizard confirmation dialog boxes



Buildings can be Added or Edited as needed by clicking on the **Add**, **Edit**, or **Remove** buttons from the first screen of the Building setup wizard.

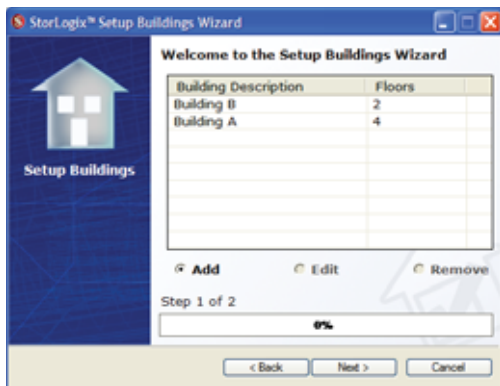


Figure 5-18 Setup Buildings Wizard Step 1 of 2 - Select a building from the list and click on Edit to change the building or Remove to delete it. Click Next to continue.

CAUTION
Elevator setup can be very complicated, especially on buildings with multiple elevators or with a combination of basement and upper levels.

Do not try to setup elevators without a written plan and sketch. It can be very confusing and cost a great deal of time and money trying to troubleshoot mistakes in the setup.

REMEMBER
It is a good idea to meet with the elevator installer and the security installer together to plan out the elevator controlled setup. This should be well in advance of the actual installation of either the elevator or the security and access control.

HINT
The lowest and highest floors serviced are very important in buildings with multiple elevators, especially in high rises where the elevators don't always service every floor. It is also important when there are basement levels along with upper levels.



Setup Elevators

The Elevator function in StorLogix is used to control elevators on the site to prevent users from accessing floors that they do not have a unit on. If the site is not using relays to control elevators, this wizard does not need to be setup.

Go to the Setup Screen in StorLogix. For more information on the Setup Screen, refer to the Setup Screen section in Chapter 3. Click on **10. Elevators**.



Figure 5-19 Setup Screen - Select 10. Elevators.

Click on the **Add** button and then **Next** to add an elevator.

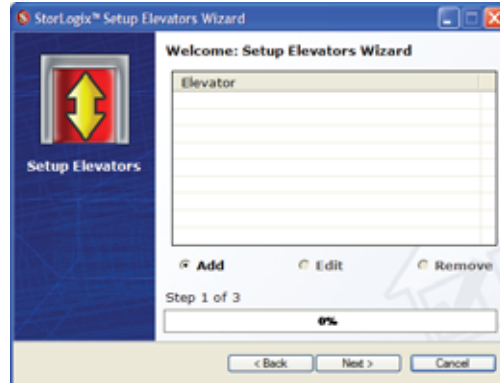


Figure 5-20 Setup Elevators Wizard Step 1 of 3 - click on Add and then Next to add an elevator to the system.

Enter the description, the building, and the floors. Click **Next**.

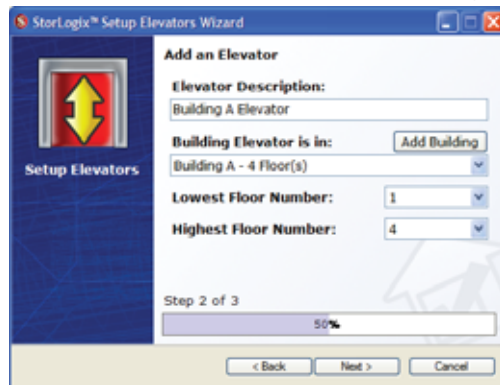


Figure 5-21 Setup Elevators Wizard Step 2 of 3 - Enter a description of the elevator that gives its location for events. Select the building that the elevator is in and select the floor serviced by that elevator. Click Next. If the buildings were not already added, click on Add Building to go to the Building Wizard.

Select the first floor with controlled access. Give the floor a good description for event location at a later date. Floor 2 might not actually be the second story of a building. See the examples in the Application note in the sidebar.

Select the relay that controls the elevator button for that floor and then click the **Add** button.

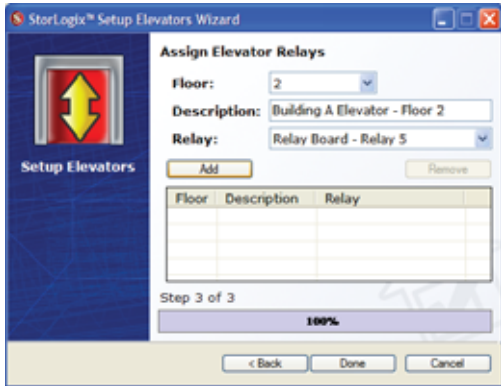


Figure 5-22 Setup Elevators Wizard Step 1 of 3 - click on Add and then Next to add an elevator to the system.

Continue adding floors and relays until all have been entered. Then, click on the **Done** button to complete the process.

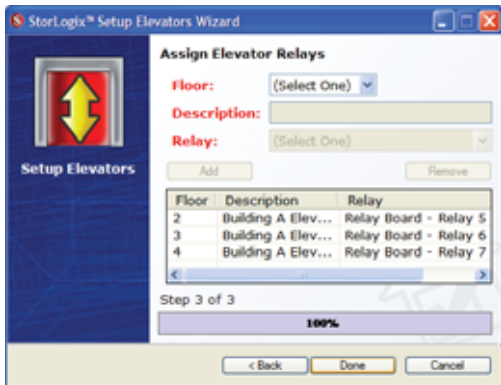


Figure 5-23 Setup Elevators Wizard Step 1 of 3 - click on Add and then Next to add an elevator to the system.

APPLICATION

Examples:

1. Building A has four stories above ground: Floor 2 would be the second floor and would be the first relay as floor one is ground level and doesn't require elevator control.
2. Building B has three stories above ground and two basement levels. Floor 1 would be the lowest basement level and be controlled by the first relay. Floor 2 would be the upper basement level and be controlled by the second relay. The ground floor would be skipped as it doesn't require elevator control. Floor 3 would be the second floor above ground and would be controlled by the third relay. Floor 4 would be the top floor and would be controlled by the fourth relay.
3. Building C has 10 floors above ground and has two elevators. Elevator 1 leaves from the ground floor and services floors 2 - 5. Elevator 2 leaves from the 5th floor but services floors 6 - 10. Elevator 1 would be setup with the lowest floor as 1 and the highest floor as 5 with Floor 2 being the second floor and connected to the first relay. Elevator 2 would be setup with the lowest floor as 5 and the highest floor as 10 with the sixth - tenth floors assigned to relays. Floor 1 and Floor 5 would not be assigned relays as they are open access floors so that users can get to the elevators.

A dialog box will appear. Click on the **Yes** button to save the Elevator.

Another dialog box will then appear to confirm that the Elevator was successfully added. Click **Yes** to continue adding and editing Elevators, click **No** to return to the Setup Screen.



Figure 5-24 Setup Elevators Wizard confirmation dialog boxes



Elevators can be Added or Edited as needed by clicking on the **Add**, **Edit**, or **Remove** buttons from the first screen of the Elevator setup wizard.

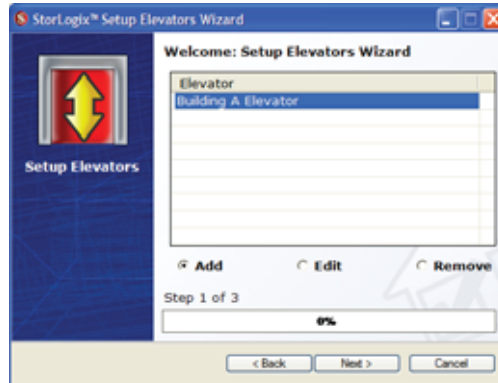


Figure 5-25 Setup Elevators Wizard Step 1 of 3 - select Add to add a new elevator or select a elevator from the existing list and click on edit to edit the elevator and Remove to remove it. Click Next to continue.

Chapter Terms

Alarm Zone	These allow a site with multiple sirens to create areas or zones where the sirens sound only for alarms that occur in that area.
Alerts	Emails that StorLogix can send based on events. See Chapter 10.
Building	For the purposes of StorLogix, any structure on a site that has its own keypad or door controller to monitor or control access or elevators.
Delay before Sounding	Advanced Alarm Zone setting that allows a delay before the alarm sounds. This can be used to allow entrance to a property and give the user time to go clear the alarm before it sounds.
Elevators	For the purposes of StorLogix, this refers only to elevators controlled by relays to limit elevator access to authorized personnel.
Lighting Area	Lighting areas are relays connected to lights in hallways, stairwells, building exteriors, or units set to come on for certain users entering that access area.
On Time	The length of time that an alarm siren will sound during day or night hours.
Pass Through Lighting Area	A lighting area that a user must go through to get to their unit that is inside a different lighting area.
Relay	A switch located in electronics used to control another device. See Chapter 4.
Start Time	The beginning of daytime or nighttime hours for a site to allow alarms to sound for different lengths of time during the day or night. See On Time.
Trip on Input	An advanced setting for lighting zones that allows them to be connected to motion sensors or other types of sensor to turn the light based on an input.
Wiegand Device	An AI Device that communicates with Wiegand Protocol Devices such as proximity card readers, fingerprint readers, or key fobs.

CHAPTER 6: ACCESS & AUTHORIZATION SETUP

- **SETUP ACCESS AREAS**
- **SETUP ACCESS AREAS - ADVANCED**
- **SETUP ACCESS LEVELS**
- **SETUP OPERATORS**

This section includes Access Areas which are the various parts of the property that are controlled by keypads or cards and Access Levels which are preprogrammed access settings for groups of users such as employees, managers, and customers. It also includes Operator setup where the users with access to the StorLogix software are setup.



Setup Access Areas

Access Areas are sections of the property where access is controlled by keypads or card readers.

Go to the Setup Screen in StorLogix. For more information on the Setup Screen, refer to the Setup Screen section in Chapter 3. Click on **11. Access Areas**.



Figure 6-1 Setup Screen - Select 11. Access Areas.

Select the Default Access Area. Click on **Edit** and then **Next**.

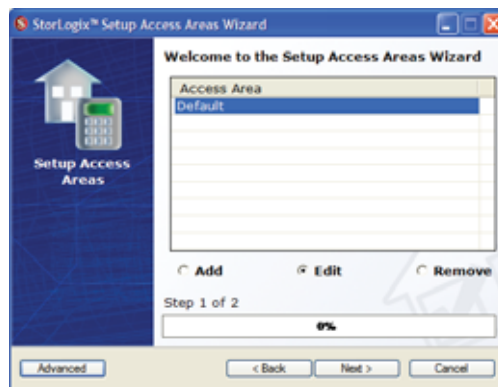


Figure 6-2 Setup Access Areas Wizard Step 1 of 2 - Select the Default Access Area from the list and click on Edit. Click Next to continue.

Give the Access Area a name and description. Select the building and floor if necessary. Click the **Done** button to complete the process.

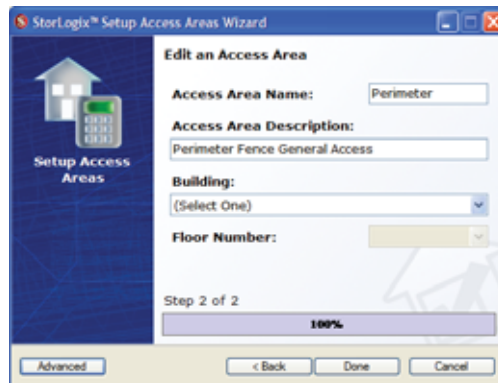


Figure 6-3 Setup Access Areas Wizard Step 2 of 2 - Give the Access Area a name and description. Be descriptive to help locate events in the future. If the area is a building or has elevator controls, enter the building name and floor number.

HINT

StorLogix has one default Access Area already created. If no other access areas are created or needed, this Access Area will represent the entire site.

If the site has a fence line with a keypad or card controlled gate, then everything within the fence line is the first access area.

If the site is only a building with keypad or card access, then the entire building is the first access area.

To be an Access Area, a location must be access controlled. If a site only has a keypad at the main gate, then the only possible access area covers the whole site.

Access Areas can be inside other areas. For example, the Access Area within the fence line is the first. Then, if each building on the site has its own keypad, then each one becomes its own access area. If the building has multiple floors and elevator controls, then each floor would be an access area of its own. Lastly, any hallways, stairwells, apartments, or units that have their own keypads would become access areas.

A dialog box will appear. Click on the **Yes** button to save the Access Area.

Another dialog box will then appear to confirm that the Access Area was successfully edited. Click **Yes** to continue adding and editing Access Areas, click **No** to return to the Setup Screen.



Figure 6-4 Setup Access Areas Wizard confirmation dialog boxes.

Continue adding Access Areas as needed for the site. Any area of the site behind a keypad or card reader is an access area. It is a good idea to set these up concentrically beginning from the outside of the site and working to the smallest area(s) within the site.

Access Areas can be Added or Edited as needed by clicking on the **Add**, **Edit**, or **Remove** buttons from the first screen of the Access Areas setup wizard.

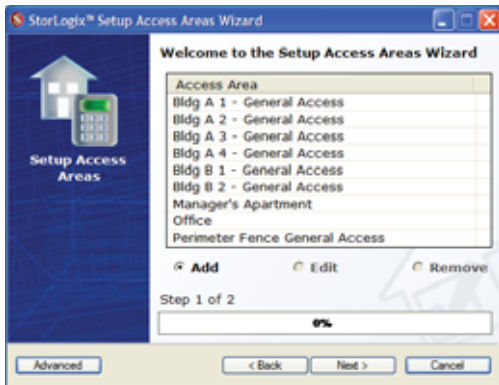


Figure 6-5 Setup Access Areas Wizard Step 1 of 2 - Select an Access Area from the list and click on Edit to make changes or Remove to delete the area.

APPLICATION

Access Areas are used in conjunction with many functions in StorLogix.

They can be used with Alarm Areas and Site Graphics to display alarms in an area that are not specific to a unit.

Access Areas must be setup when using elevator controls. Each controlled floor is an alarm area.

When used with Access Levels, it is possible to keep certain users out of areas where they are not authorized or limit the hours that they can get into certain areas. A single user could have multiple Alarm Areas that they have access to, with different hours of access for each.

Setup Access Areas - Advanced

Access Areas have advanced features that can be setup.

If the StorLogix Preferences were setup with 'Advanced Menus Always On', then the advanced steps will already be visible. If not, from Step 2 of the Access Area setup process, click on the **Advanced** button at the bottom left corner of the field. This adds advanced Steps 3, 4, & 5. Click the Next button from Step 2 to get to this Advanced screen.

Lighting Area: A lighting area can be associated with an Access Area so that anyone entering that access area will activate the lighting area. Select a lighting area from the drop down list if desired.

Maximum Users in Area: The number of users can be limited in a particular access area. Select a number from the drop down list or leave it as unlimited.

Rearm Wait Time: The amount of time after an area has been entered before the area is cleared and the alarm is reset.

Area Suspended: If this box is checked, then no one can enter the area, although anyone with valid access is allowed to exit the area if they are already inside.

Area in Lockdown: If this box is checked, then all access is blocked. No one can enter or exit the area at all.

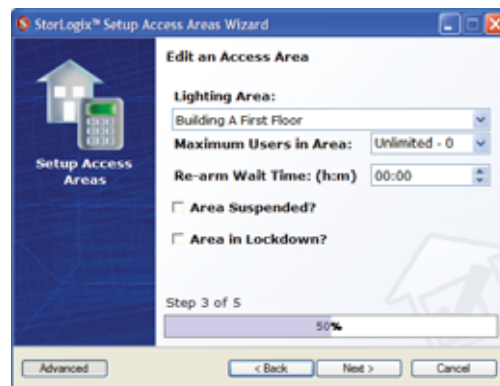


Figure 6-6 Setup Access Areas Wizard Advanced Step 3 of 5 - Select the advanced functions and click on Next to continue.

APPLICATION

Maximum Users in Area could be used to comply with fire department restrictions on the maximum number of people in a certain area.

CAUTION

Rearm Wait Time should only be used in areas where the user is expected to pass through fairly quickly and the site does not want them to remain in the area. An example of this would be a monitored stairwell or hallway with access control at both ends. This could be used to help prevent crime by making sure that the person passes through the area and does not stay in there.

This should not be activated for any area that a person could potentially stay in for awhile. If they stayed in there past the Rearm wait time, they would be cleared out of the area and the alarm would be reset, setting off the siren. If anti-passback is being used, then they could potentially be locked in the area. If Lighting controls are being used, the lights could turn off.

Access Areas can be associated with alarm inputs to allow motion sensors, glass break sensors, and door contacts to be placed in areas that are not units.

Select Inputs from the drop down list and click the **Add** button. Multiple inputs can be added to an Access Area.

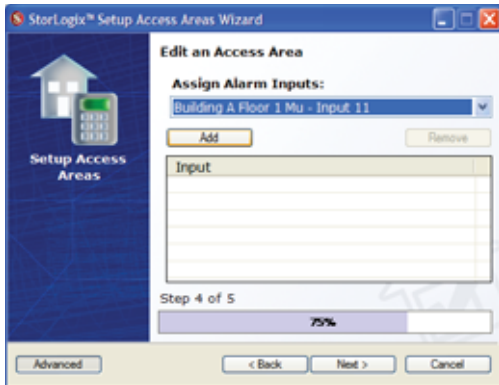


Figure 6-7 Setup Access Areas Wizard Advanced Step 4 of 5 - Select alarm input and click on Add if alarm inputs are being associated with the area. Keep adding alarm inputs until all applicable ones are added, then click Next.

Alarm Zones can be associated with Access Areas. Select an Alarm Zone from the drop down list and click the **Add** button. Multiple Alarm Zones can be associated with an access area.

Click **Done** when advanced setup is complete.

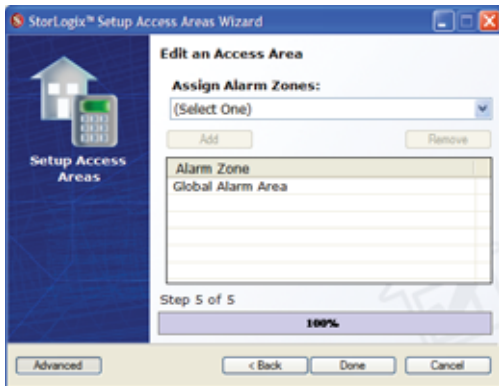


Figure 6-8 Setup Access Areas Wizard Advanced Step 5 of 5 - Select the alarm zone to associate with the access area, if applicable.

APPLICATION

Adding alarm inputs to an Access Area allows motion sensors to be placed in hallways and stairwells, glass break sensors to be placed on building windows, and door switches to be placed on doors that are not on rentable units.



Setup Access Levels

Access Levels are preset authorizations that combine Time Schedules and Access Areas. These are setup to make adding users easier.

Go to the Setup Screen in StorLogix. For more information on the Setup Screen, refer to the Setup Screen section in Chapter 3. Click on **12. Access Levels**.



Figure 6-9 Setup Screen - Select 12. Access Levels.

Select the Default Access Level, click on **Edit** and click on **Next**.

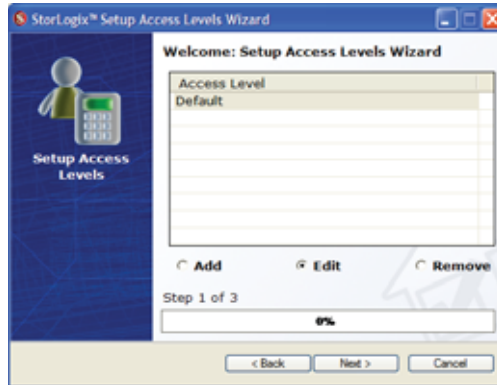


Figure 6-10 Setup Access Levels Wizard Step 1 of 3 - Select the default access level from the list, click on Edit and then Next.

Input an Access Level Description. Select a required level on-site if desired and click **Next** to continue.

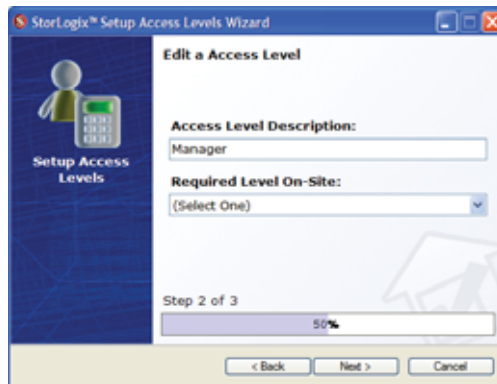


Figure 6-11 Setup Access Levels Wizard Step 2 of 3 - Make the Access Level Description very descriptive to make it easier to select the right one later.

???????? HINT

StorLogix has one default Access Level. This area should be renamed and setup to represent an Access Level for the site.

In most cases a site will only have 2 or 3 Access Levels; one for customers, one for employees, and possibly one for managers.

APPLICATION

Using the Required Level On-Site function, StorLogix can require that a user of a certain level be on-site (or in a certain Access Area) before letting the user have access. This could be used to require that a Manager be logged into the office before an employee can gain access to the office. Or, it could require that an employee be logged onto the site before any customers are allowed in the front door.

Select an Access Area that users in this access level will have access to. Then select a Time Schedule during which they will have access to the Access Area. If they have a unit in the area, check the Unit in Area? box. Then click the Add button.



Figure 6-12 Setup Access Levels Wizard Step 3 of 3 - Select the Access Area and Time Schedule and Unit in Area if desired. Click Add to add to the list for this Access Level. Multiple combinations may be entered for the same level. Click Done when finished.

Continue entering Access Areas and Time Schedules for this Access Level until all approved access for this Access Level is completed.

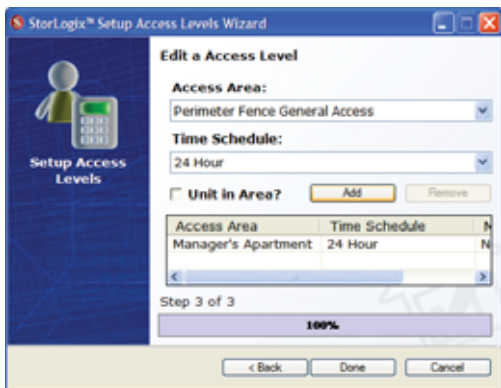


Figure 6-13 Setup Access Levels Wizard Step 3 of 3 - Select the Access Area and Time Schedule and Unit in Area if desired. Click Add to add to the list for this Access Level. Multiple combinations may be entered for the same level. Click Done when finished.

Click **Done** to complete the process.

A dialog box will appear. Click on the **Yes** button to save the Access Level. Another dialog box will then appear to confirm that the Access Level was successfully edited. Click **Yes** to continue adding and editing Access Levels, click **No** to return to the Setup Screen.



Figure 6-14 Setup Access Levels Wizard confirmation dialog boxes.

APPLICATION

If the site has elevator controls with multiple Access Areas or more than one building AND customers potentially could have units in more than one of these areas; create an Access Level that includes all of the areas but has the Unit in Area box checked. This gives the customer that is placed in that Access Level access to any areas where they have a unit, but prevents them from going into other areas.

HINT

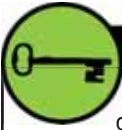
Access Levels are used to control access by performing checks as a user enters their code at a keypad or presents a card.

The system first checks if the code is valid and the user is not suspended.

Then it checks the Access Level in this order:

1. Is a required level on-site?
2. Is the user allowed in this area?
3. Is the user allowed during this time?
4. Does the user have a unit in this area?

If all is OK, then access is allowed.



????????? HINT

StorLogix has two default operators that are created with every setup. The default Administrator is always automatically created. A second administrator is named and created during the initial setup. Generally, this is the first person who setup StorLogix.

It is a good idea to add a new operator for any employee who will be using the software. This allows any functions they perform in the system to be tracked and it also allows them to be locked out of the system when they leave the company.

Combined with Security Levels that were setup in Chapter 3, operators can have different privileges in the system.



CAUTION

For security reasons, any password should generally be 4 or more characters in length. To prevent security breaches from someone guessing a password, all passwords should contain a mixture of numbers, letters, and other characters. Passwords in StorLogix can be up to 15 characters in length and are NOT case sensitive.

Long passwords may be difficult to remember, especially with numbers or characters added in. However, if you use a word like Falcon as a password and just change the letter 'l' to a number '1' as in Fa1con, then it becomes easy to remember and still secure.

Never use birthdays, children's names, hobbies, phone numbers or other similar things as passwords as they are very easy to guess.



Setup Operators

Operators are users that have access to the StorLogix software. Operators are added and edited in this area based on Security Levels that were setup in Chapter 3.

Go to the Setup Screen in StorLogix. For more information on the Setup Screen, refer to the Setup Screen section in Chapter 3. Click on **13. Operators.**



Figure 6-15 Setup Screen - Select 13. Operators.

To add a new operator, click on **Add** and then click on the **Next** button.

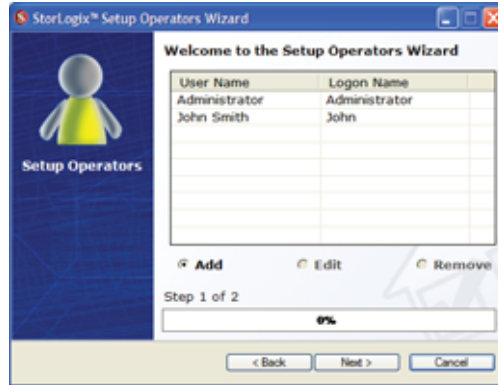


Figure 6-16 Setup Operators Wizard Step 1 of 2 - to Add a new operator, click Add and Next.

Enter the Name of the Operator being added. Assign an Operator Logon Name and Password and select a Security Level Click **Done**.



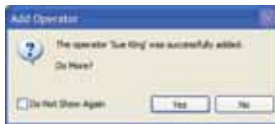
Figure 6-17 Setup Operators Wizard Step 2 of 2 - Enter the operator information and click Done.

A dialog box will appear. Click on the **Yes** button to add the Operator.

Another dialog box will then appear to confirm that the Operator was successfully added. Click **Yes** to continue adding and editing Operators, click **No** to return to the Setup Screen.



Figure 6-18 Setup Operators Wizard confirmation dialog boxes



Operators can be Added or Edited as needed by clicking on the **Add**, **Edit**, or **Remove** buttons from the first screen of the Operators setup wizard.

To Edit the first and last name of an existing operator, go to the User Operations screen and edit the User. This is covered more in depth in the StorLogix Operations manual.

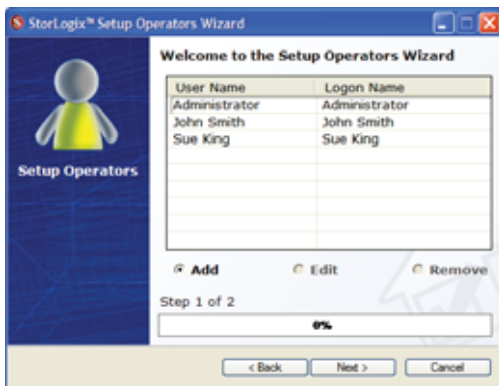


Figure 6-19 Setup Operators Wizard Step 1 of 2 - Select an operator from the list and click Edit to change them or click remove to delete them from StorLogix.

CAUTION

The Administrator password can be changed, but don't lose it. All operators can be removed but the Administrator, but if that password is lost, it can't be retrieved.

REMEMBER

All operators are users, but not all users are operators. Users are anyone with access to the site. Operators are users with access to the StorLogix software.

Chapter Terms

Access Areas	Parts of the site where access is controlled by keypads or Wiegand devices. Access Areas can be inside other Access Areas. For example, most sites will have a Default Access Area that is the entire site inside the fence line. Within that access area may be several buildings, each with their own keypads for access. Inside each building may be several floors, each with their own keypads for access. Inside each floor may be several rooms, each with their own keypads for access. These would all be access areas.
Access Controlled	Preventing access to or egress from an enclosed area by using a fence or wall with a gate or door in it. Persons wanting to enter or exit the enclosed area must enter a code or present a card at a device controlling the door or gate.
Access Levels	Used to add groups of people with similar access privileges. For example, if a site has managers, employees, and customers with two different types of access, they can setup access levels to make it easier to add each of these types of users without having to remember all of the variables every time one is added. Access Levels are a combination of Access Areas and Time Schedules.
Administrator	User with full rights to setup or change any part of StorLogix.
Area in Lockdown	All access is blocked. No one can enter or exit the affected area at all.
Area Suspended	No one can enter the area affected, but anyone with valid access is allowed to exit the area if they are already inside it.
Fence line	The enclosure for access control. May be a wall, fence, or any other barrier that forces entry to a site through a controlled door or gate.
Logon ID	ID used with password to gain access to the software. Usually the person's name.
Maximum Users in Area	The number of users that are allowed inside an access area at any one time based on a count of the number of users entering the area minus the users that have left the area. Anyone trying to enter the area once the maximum number is reached will be denied access.
Off-Site	For the purposes of StorLogix, this is the area outside of the fence line, that is the area that is not inside an access area. Essentially, it is the rest of the world other than the site.
On-Site	The area within the fence line of a site that is access controlled. For StorLogix purposes, this is anything inside the main Access Area.
Operators	A User that has access to the StorLogix software. Generally an employee of the site.
Password	A unique private identifier from 1 to 15 characters that is used along with the Logon ID for an Operator to gain access to the StorLogix software.
Rearm Wait Time	The amount of time after an an area has been entered before users in the area are cleared and the alarm is reset. This is an optional advanced function of Access Areas and is generally used for stairwells or other areas that users must pass through and should not remain in.

Required Level On-Site	An optional function of Access Levels that can require someone of a higher level be on-site before a person of a lower level is allowed access. For example, the system could require that a manager be logged into an office area before an employee could gain access or an employee must be logged on-site before a customer can gain access to the front door.
Security Level	These are the various preset levels of access permissions and privileges for the computer operators, including which functions in StorLogix they have access to.
Unit in Area?	An optional limitation to Access Levels to allow a user access to any area in which they have a unit, but not to any area where they do not have units. Generally used with elevators or with multiple access controlled buildings on a site so that customers with units in multiple buildings or on multiple floors can access all of their units with one entrance code.

CHAPTER 7: UNIT SETUP

- **SETUP UNITS**
- **SETUP INPUTS TO UNITS - BASIC**
- **SETUP INPUTS TO UNITS - ADVANCED**
- **IMPORTING UNITS AND INPUTS TO UNITS**
- **EXPORTING UNITS AND INPUTS TO UNITS**

This chapter covers setting up units and inputs to units which are generally the door alarms for the units. The manual ways to enter these items are covered along with importing an alarm file to setup units and inputs to units automatically.



Setup Units

Units are storage spaces, lockers, parking spaces, offices, rooms, suites, mailboxes or other areas that are generally rented to clients. They can also include manager units, apartments, storage sheds, dumpster areas, security closets, and any other enclosed area that might be monitored.

Go to the Setup Screen in StorLogix. For more information on the Setup Screen, refer to the Setup Screen section in Chapter 3. Click on **14. Units**.



Figure 7-1 Setup Screen - Select 14. Units.

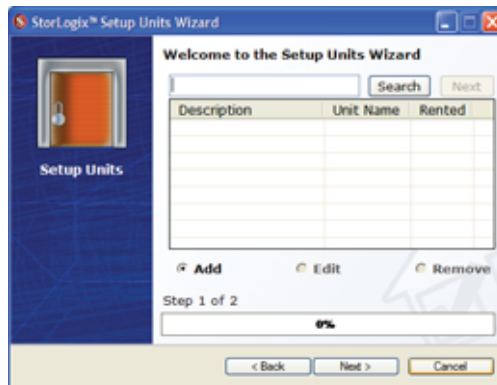


Figure 7-2 Setup Units Wizard Step 1 of 2 - select Add to add New Units. Click Next to continue.

To add new units, click on **Add** and then click on the **Next** button.

Input the Unit information for the first unit or group of units.

Unit Name: Enter the first unit name. Unit Names can be up to 10 characters. This is generally the number that is painted on the door. If the site is using PTI Site Graphics, then the number must match the unit number in the Site Graphics program or the Site Graphics will not function correctly.

Unit Description: The unit description field allows more information, up to 50 characters long, to be entered for site reference purposes.

Rearm time: This serves two functions. 1) It is the time from the moment that they close their unit door until the unit alarm is rearmed to protect their unit. 2) It also serves as the amount of time that they have from the moment that they log onto the site to open the unit door. If they do not open the unit door before the timer runs out, then the alarm will sound when they do open the door. See Caution on the sidebar.

Access Area: This allows the unit to be associated with the access area that they are in.

Lighting Area: This allows the unit to be associated with a lighting area so that the lights come on when they log onto the site. This is only used if lights are controlled by StorLogix.

Stop Rearm Timer with Door Open: This should generally be checked. This allows the rearm timer to stop counting down while a user has their door open and reset the countdown to the full rearm time once they shut the door. This would only be unchecked if the site wants to limit how long the user can be in the unit.

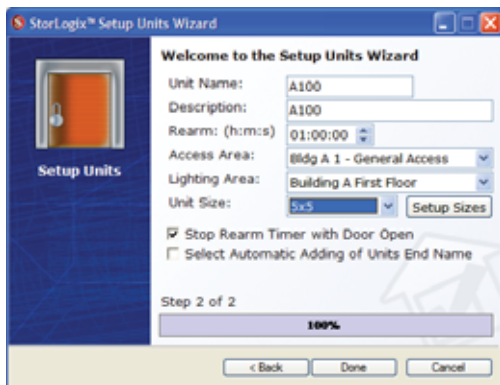


Figure 7-3 Setup Units Wizard Step 2 of 2 - Input Unit Information

????????? HINT

In most cases the unit name will be a number (such as 100) or a number preceded by a building or floor identifier (such as A100 or 2-100).

Use identifiers could also be used (such as RV-100 for RV space or Box 100 for mailboxes).

Names or words could also be used to differentiate parts of the site or actual building names (such as Pine 100 or 1st Ave 100).

CAUTION

Rearm Time must be set high enough to allow the user to get to their unit, including time for them to do things such as unload the car, get a cart, go to the office and pay their bill, etc. PTI suggests a minimum of 30 minutes to 1 hour if rearm time is being used, but this will vary based on the site layout and usage. Generally, it is a good idea to figure out the amount of time it takes to walk from the parking lot space farthest from the building to the unit that is farthest away from the parking lot. Then add additional time for any other things the user might do on the way.

When the user leaves the site, their unit alarm will be unarmed during this time unless they log out of the site.

Leaving Rearm time set to 00:00:00 will turn off the Rearm Time function. If this is the case, then the alarm can be rearmed by the user logging off the site or by Clearing All On-Site Users on the StorLogix Toolbar.

After entering information about the first unit, multiple units can be added in consecutive number order by clicking on the Select Automatic Adding of Units. This will add a range of units between the first Unit Name at the top of the page and the Unit Name entered in the field below this checkbox.

For example, if the Unit Name at the top of the page is A100 and A105 is input in the field below this box, then StorLogix will automatically add 6 units (A100, A101, A102, A103, A104, and A105) to the system. This will only work if the Unit Name ends with a number.

All units added in series this way will have the same Rearm Time, Access Area, and Lighting Area as the first one.

Click **Done** to add the units.

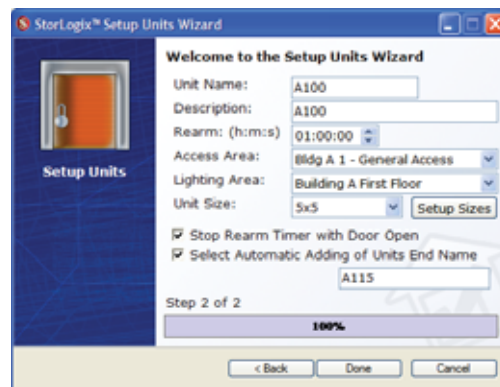


Figure 7-4 Setup Units Wizard Step 2 of 2 - Automatically adding consecutive units. Click Done to continue.

A dialog box will then appear to confirm that the Units were successfully added. Click **OK** to confirm.



Figure 7-5 Setup Units Wizard Step 1 of 2 - select Add to add New Units. Click Next to continue.

Units can be edited or removed as needed by clicking on the unit and then selecting **Edit** to change the unit information or **Remove** to delete the unit. Click Next to continue.

The unit list can get quite long and make it difficult to find units to edit or remove. Type a unit name in the search field and click **Search**.

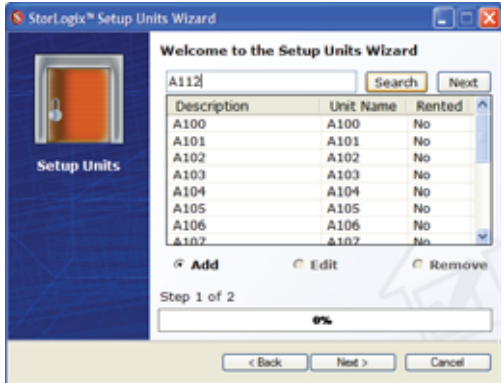


Figure 7-6 Setup Units Wizard Step 1 of 2 - selecting a unit or range of units to edit or remove. Searching for units.

The search can be for any part of the Unit Name, Description, or for the Rented status. Type any part of the information in the search field and click on Search. Click the Next button to select the next unit with the same information that was searched for.

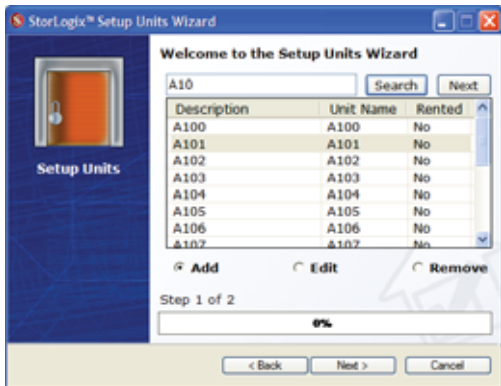


Figure 7-7 Setup Units Wizard Step 1 of 2 - Searching for units with partial information.

Click on any field heading to sort the list alphanumerically.

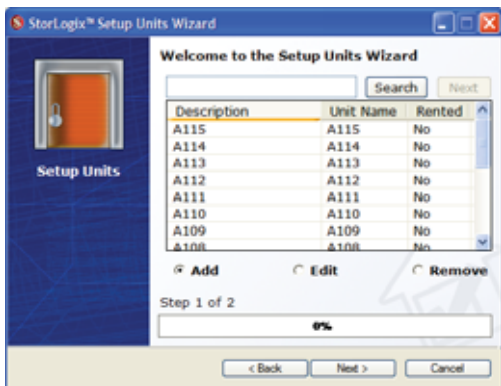


Figure 7-8 Setup Units Wizard Step 1 of 2 - Sorting the lists alphanumerically. Click on Description, Unit Name, or Rented field headings to sort the list alphanumerically by that field.



Searching for partial information lets the search be broader, helping to find ranges of units. For example, in the site shown, searching for units A10 would bring help to find any units from A100 to A109. The search would find A100 first and then by clicking Next, it would find A101, A102, etc.

To select a unit to edit or remove, click on the unit in the list. A range of units can be selected by clicking on the first unit in the list, holding down the shift key and selecting the last unit that is desired. This will select every unit within that range.

Multiple units can also be selected by clicking on the first unit in the list and then hold down the Ctrl key while clicking on any other units desired. This allows multiple units that are not consecutive to be selected together.

With multiple units selected, click on Next and complete Step 2 of 2 to make all of the units have the same formatting.



Setup Inputs to Units - Basic

Inputs to Units are alarm switches that are associated with specific units. This may be door switches on the unit door or motion sensors inside the unit.



Figure 7-9 Setup Screen - Select 15. Inputs to Units.

Go to the Setup Screen in Storlogix. For more information on the Setup screen , refer to the Setup Screen section in Chapter 3. Click on **15. Inputs to Units**.

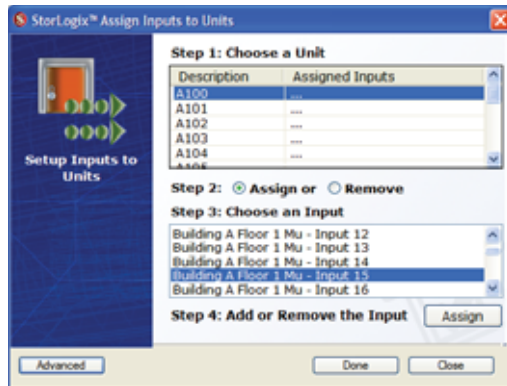


Figure 7-10 Setup Inputs to Units Wizard Step 1 of 1 - select a unit from the top list, choose assign or remove, then select an input from the bottom list. Then select the Assign or Remove button.

???????? HINT

If it is only necessary to assign or remove a few units, use the basic screen as shown on this page.

If it is necessary to assign a large number of units such as when the site is being setup, click on the **Advanced** button and use the steps on the following pages.

Individual Units can be have inputs assigned or removed easily in the basic screen. If it is necessary to assign a large number of units such as when the site is first being setup, click on the **Advanced** button and use the information on the following pages.

To add or remove individual units from the basic view:

- Step 1: select a unit from the Choose a Unit list by clicking on it.
- Step 2: select Assign or Remove input.
- Step 3: select the input from the Choose an Input list by clicking on it.
- Step 4: Click on the Assign or Remove button.

When finished click on the **Done** button at the bottom of the window.

Setup Inputs to Units - Advanced

If a lot of units need to be added, the advanced wizard is much easier to use.

If the StorLogix Preferences were setup with 'Advanced Menus Always On', then the advanced step will already be visible. If not, from Step 1 of the Setup Inputs to Units wizard, click on the **Advanced** button at the bottom left corner of the field.

Select the first Mux - Channel input from the first list by clicking on it. Select the Unit Name that the input is connected to from the second list by clicking on it. Then click the **Assign** Button. Continue doing this until all Inputs and Units are matched up.

When all units and inputs are matched up, click on the **Done** button.

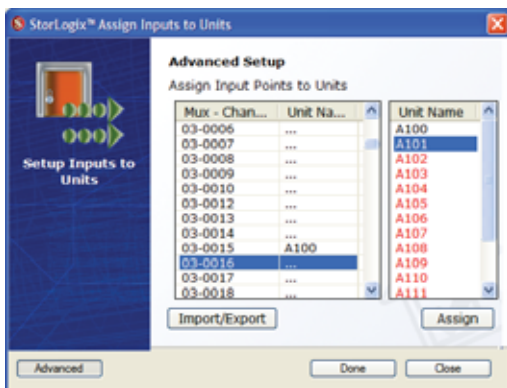


Figure 7-11 Setup Inputs to Units Wizard Step 1 of 1 - select a unit from the top list, choose assign or remove, then select an input from the bottom list. Then select the Assign or Remove button.

A dialog box will appear. Click on the **Yes** button to save the Inputs to Units.

Another dialog box will then appear to confirm that the Inputs to Units were successfully edited. Click **Yes** to continue adding and editing Inputs to Units, click **No** to return to the Setup Screen.



Figure 7-12 Setup Inputs to Units Wizard confirmation dialog boxes



APPLICATION

Often, the Units go in numeric order along with the Mux and Channel inputs. If this is the case, assign the first unit as shown above. Then, click on the next Unit name and click assign. StorLogix will automatically assign the next Mux and Channel input to that unit. Continue doing this as long as they go in numeric order.

If this method is used, the Mux and Channel assignments will be highlighted in yellow until they are saved by clicking on the Done button.

Importing Units and Inputs to Units

If the site already had an existing Falcon system or if the installer is comfortable setting up an alarm file, then units and inputs to units can be imported together by importing an alarm.alm file. From the Advanced Setup view of the Assign Inputs to Units Wizard, click on the **Import/Export** button.

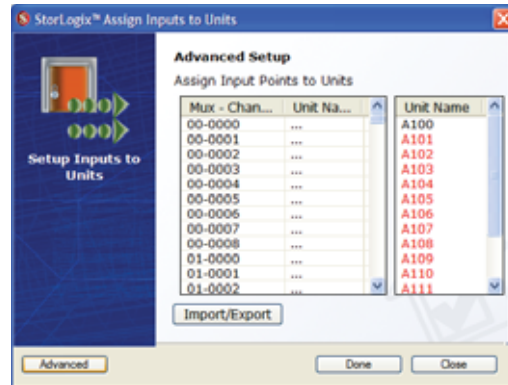


Figure 7-13 Setup Inputs to Units Wizard Importing Alarm Files.

Select the Import button. Two options will appear to Automatically Add Units and Automatically Add Input Points. If units have already been added, uncheck the Automatically Add Units. To automatically add units, check the box. Generally, Automatically Add Input Points will need to be selected. Then, click **Browse**.

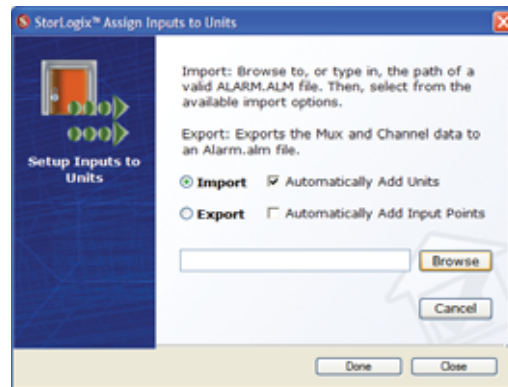


Figure 7-14 Selecting the Import Function.

Browse for the alarm.alm file. Select it and click the **Open** button.



Figure 7-15 Browsing for the Alarm.alm File.

CAUTION

If an alarm file is imported to setup units and inputs to units, then the installer must still go into the Setup Units wizard to associate units with Access Areas and Lighting Areas as well to set the Rearm Time.

HINT

If the site already had Falcon 2000, then the alarm file will usually be found in the C:\F2000 folder.

If the site did not have Falcon 2000, but was interfaced to an accounting software, then the alarm file will often be found in the C:\PTI file.

If the file isn't in either of these two places, do a search for "alarm.*" or "*.alm".

The Import screen will now show the file path in the field next to the Browse button. Click on **Check Import** to continue.

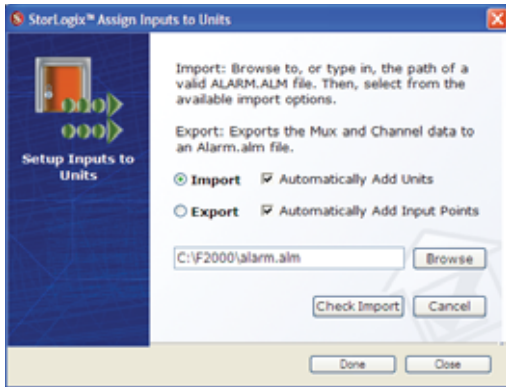


Figure 7-16 Setup Inputs to Units Wizard Importing Alarm Files. Select the file path and click on Check Import.

The Check Import Screen will now come up. Scroll down through the lines to check the import. Any lines highlighted in yellow or red need to be corrected in the system. When all is correct, click on **Save Import**.

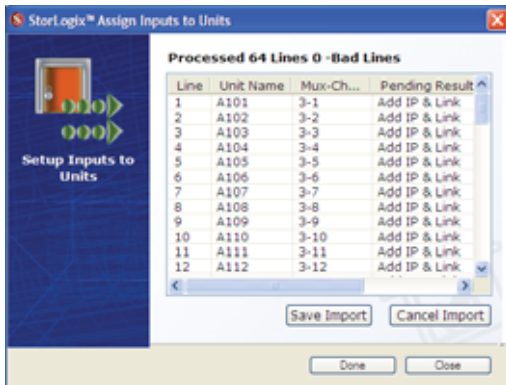


Figure 7-17 Checking the Import.

If the units being added were new, the Rearm Time, Access Area, and Lighting Area information must be entered for these units. This screen will come up. Make any necessary changes and click **Done** when finished.

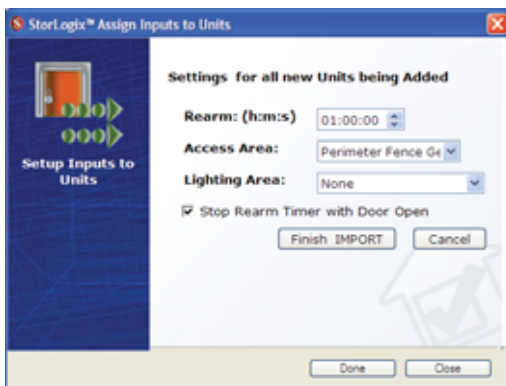


Figure 7-18 Browsing for the Alarm.alm File.

APPLICATION

Any changes made to the Rearm Time, Lighting Area, or Access Area here affect all of the new units being added. If some of the units are in other areas, go to the Setup Units wizard to make changes as necessary.

Exporting Units and Inputs to Units

It is always a good idea to backup the alarm information for the site. Losing this information can be very costly as the information will need to be rebuilt by opening every alarmed door on the site. This is expensive and time consuming. To prevent the need for this, always save a backup of the alarm information. From the Advanced Setup view of the Assign Inputs to Units Wizard, click on the **Import/Export** button.

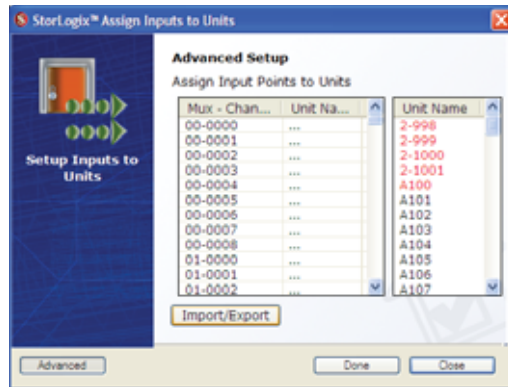


Figure 7-19 Setup Inputs to Units Wizard Exporting Alarm Files.

Select the Export function and then click on the **Browse** button.

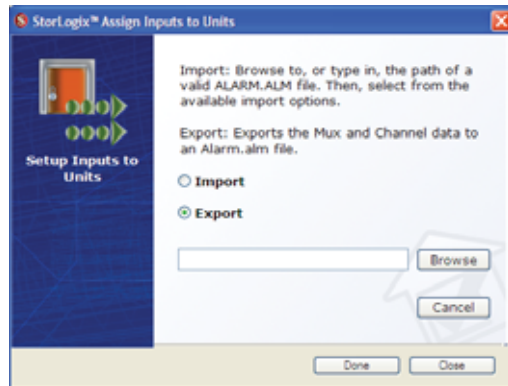


Figure 7-20 Selecting the Export Function.

Browse to find the location where the file will be saved and click the **Open** button.



Figure 7-21 Browsing for the location to save the Alarm.alm File.



ALWAYS KEEP A BACKUP COPY OF THE ALARM.ALM.

Computer theft, hard drive crashes, operator error, network problems, viruses, physical damage, flooding, fire and a number of other problems could cause the loss of an alarm file.

PTI strongly recommends that a hard copy of the alarm.alm be burned onto a CD or DVD and be stored in a safe location offsite.

The installer should ALSO keep a copy of the alarm.alm file along with the site wiring diagram and other site information for future service and maintenance.

The Export screen will now show the file path in the field next to the Browse button. Click on **Export** to continue.

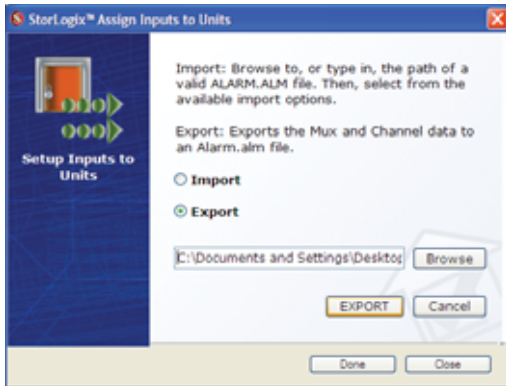


Figure 7-22 Setup Inputs to Units Wizard Exporting Alarm Files. Select the file path and click on Export.

A dialog box will now appear confirming the Export of the Alarm.alm file. The dialog box will show the path where the file was saved. Click **OK**. A copy of this file can be kept on the computer, but PTI strongly advises that a copy be burnt onto a CD or DVD and kept in a safe location offsite so that the alarm file can be reloaded again if necessary. See Caution in the sidebar on the previous page.



Figure 7-23 Export Alarm.alm confirmation dialog box.



REMEMBER

The alarm file is absolutely necessary for the operation of alarms in the system. If the computer is ever changed or a new one installed, be sure to copy the alarm.alm from the old computer to the new one.

If the computer ever needs to be changed, it is a good idea to contact PTI Technical Support for advice on what files to copy and save as well as what files to be sure to wipe off the old computer before getting rid of it.

Chapter Terms

Access Areas	Parts of the site where access is controlled by keypads or Wiegand devices. Access Areas can be inside other Access Areas. For example, most sites will have a Default Access Area that is the entire site inside the fence line. Within that access area may be several buildings, each with their own keypads for access. Inside each building may be several floors, each with their own keypads for access. Inside each floor may be several rooms, each with their own keypads for access. These would all be access areas.
Alarm File or alarm.alm	This is the file that associates the unit number painted on the door (unit name) with the multiplexer address (Device ID) and channel or input number.
Browse	To search on a computer using the explore feature to find the location that a file is at or should be save to.
C:\	The C drive on a computer. Usually this is the hard drive of the computer where programs and other information is stored, but occasionally, the computer is setup with a different letter of the alphabet designating the hard drive.
Export	To send data from one program to another. For example, to save a copy of the alarm file created in StorLogix to another location.
Import	To use data created by another application. For example, to use an alarm file created in Falcon 2000 or word pad to input the unit information into StorLogix.
Inputs to Units	Inputs to Units are alarm switches that are associated with specific units. This may be door switches on the unit door, motion sensors inside the room, or photobeams across an RV space.
Lighting Area	Lighting areas are relays connected to lights in hallways, stairwells, building exteriors, or units that are set to come on for certain users entering that access area.
Off-Site	For the purposes of StorLogix, this is the area outside of the fence line, that is the area that is not inside an access area. Essentially, it is the rest of the world other than the site.
On-Site	The area within the fence line of a site that is access controlled. For StorLogix purposes, this is anything inside the main Access Area.
Rearm Time	In connection with Units, this serves two functions: 1) It is the time from the moment that the user closes their unit door until the unit alarm is rearmed to protect the unit. 2) It also serves as the amount of time that the user has from the moment that they log onto the site to open the unit door. If they do not open the unit door before the timer runs out, then the alarm will sound when they open the door. Rearm time must be set high enough to allow the user to get to their unit, including time for them to do things such as unload the car, get a cart, go to the office, and pay their bill, etc. Generally, it is a good idea to figure out the amount of time it takes to walk from the parking lot space farthest from the building to the unit that is farthest away from the parking lot. Be sure to add some additional time for any other things the user might do on the way.
Setup Units	Function in StorLogix to enter the units for the site.

Unit	Units are storage spaces, lockers, parking spaces, offices, rooms, suites, mailboxes, and other areas that are generally rented to clients. However, they can include manager units, apartments, storage sheds, dumpster areas, security closets, and any other enclosed area that might be monitored.
Unit Description	A 50 character field that allows more information about the unit for site reference purposes.
Unit Name	Generally, this is the number that is painted on the door of the unit or otherwise associated with the unit to uniquely identify it. In most cases the unit name will be a number (such as 100) or a number preceded by a building or floor identifier (such as A100 or 2-100). Other identifiers and words can be used base on use or location (such as RV-100, Box 100, Pine 100, or 1stAve 100). This field is limited to 10 characters and MUST match the unit name in site graphics.

CHAPTER 8: DEVICE CONFIGURATION SETUP

- **SETUP DEVICE PROPERTIES**
- **SETUP DEVICE PROPERTIES - ADVANCED**
- **SETUP FALCON XT**
- **SETUP FALCON XT - ADVANCED**

This section covers the individual setup of each AI Device and the Falcon XT. The advance functions in these wizards allow many features that are customizable to the facility.



Setup AI Device Properties

AI Device Properties defines the controls for AI Devices including operating mode, access areas, and relays.

Go to the Setup Screen in StorLogix. For more information on the Setup Screen, refer to the Setup Screen section in Chapter 3. Click on **16. AI Device Properties**.



Figure 8-1 Setup Screen - Select 16. AI Device Properties.

Select a device from the list. Click on **Edit** and then the **Next** button.

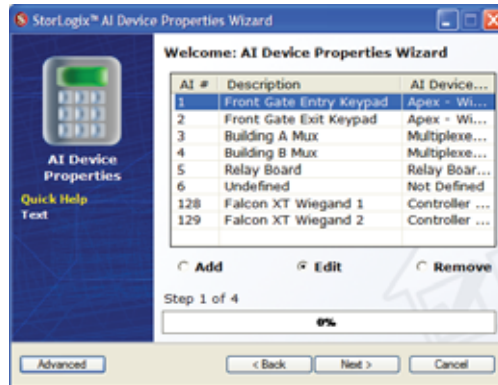


Figure 8-2 Setup AI Device Properties Wizard Step 1 of 4 - Select an AI Device from the list, click Edit and then the Next button.

Select the type of AI Device from the drop down list and input a description. Click Next to Continue.



Figure 8-3 Setup AI Device Properties Wizard Step 2 of 4 - Select the type of AI Device and then enter a description for the device. Be descriptive to help with event location in the future. Click Next to continue.

Note that the current device status shows Online or Offline on this screen.

???????? HINT

AI Devices could be added from scratch in this Wizard if the Falcon XT and AI Devices are not already connected, however, the output relays and alarm inputs would not be automatically setup in the previous setup steps.

StorLogix is powerful, saving a lot of steps by automatically setting up devices if they are already connected and powered. For this reason, PTI recommends that all AI Devices be connected to the Falcon XT and the Falcon XT be connected to the StorLogix computer before beginning the entire setup process.

Select the FROM and TO Access Areas. This tells the device what message to use when access is granted and helps with the Anti-passback functions covered later. Then select the function mode, elevator (if applicable), and operating mode. More information on the Function Mode and Operating Mode can be found in the sidebar to the right. Click **Next** to continue.



Figure 8-4 Setup AI Device Properties Wizard Step 3 of 4 - Select the From and To Access Areas, Function Mode, Elevator if applicable, and the Operating Mode. Click Next to continue.

Select the relay(s) to trip when a user enters a valid access code. Initially, this will be the relay connected to the gate or door strike to open it. Other relays can be used to activate lights or virtual relays and scripts when the valid access is entered. Then click **Done**.

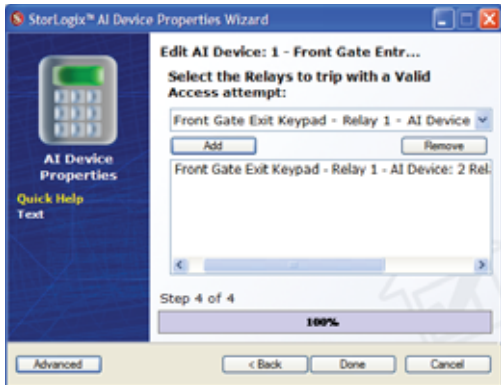


Figure 8-5 Setup AI Device Properties Wizard Step 4 of 4 - Select the Relay(s) to trip with a valid access. In a UL recommended setup, the relay to open a door or gate should always be on the secure interior side of the door or gate. Therefore, in an entrance gate situation, the exit keypad should be wired to the gate operator and the entrance keypad should be programmed to trigger the exit keypad relay.

A dialog box will appear to confirm the AI Device is updated. Click Yes to edit more AI Devices or click No to return to the setup screen.

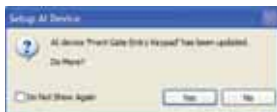


Figure 8-6 Setup AI Device Properties Wizard confirmation dialog box.

APPLICATION

Access: This is the function is for most keypads or Wiegand devices that are used to enter an area or exit an area (gates or doors)

Check In/Out: This function allows a keypad to be setup so that everyone must check-in at this location (such as in the office) before they can use any other keypad or open any alarmed door on the site. They must also check out at this keypad.

Elevator: This function is for any keypad or Wiegand used to control an elevator.

Time & Attendance: Coming soon, this function will allow a keypad or Wiegand to be used as a time clock for employees.

Entry/Exit: This is used primarily when there is only one keypad on a site with alarms. Users must come and enter their code at this keypad to turn off the alarm at their unit. The second time they enter their code at this device, it turns the alarm back on.

PayXpress Only: Used to give clients a place to pay their bill quickly and easily.

Code Only: For keypads that do not have cards, this lets the keypad function by using the touchpad.

Card Only: For keypads with card readers, it lets the keypad accept access using just a card.

Card+Pin: For Apex keypads with card readers, this high security feature requires a card and a pin number to prevent stolen cards from gaining access.

Setup AI Device Properties - Advanced

AI Device Properties have advanced features that can be setup.

If the StorLogix Preferences were setup with 'Advanced Menus Always On', then the advanced steps will already be visible. If not, from Step 4 of the AI Device setup process, click on the **Advanced** button at the bottom left corner of the field. This adds advanced Steps 5-10. Click the **Next** button from Step 4 to get to this Advanced screen.

Timed Operating Mode: This allows the device to work differently at different times of the day. Select an Operating Mode and then **Select the Schedule for Timed Operation** in the field below it. See the application note in the sidebar.

Passback Setting: These rules are used if the site is using Anti-passback. Anti-passback is a higher security feature used to help keep tighter control on access and force users to log into and out of areas for tracking purposes. It works by preventing users getting into areas if they did not log out of the area last time or if they are not in the logical previous area. For example, tailgated another person onto the site without using their own access card or code and the User must be On-site rule is activated, then the system would not allow them access to any keypad controlled building on the site because they are not logged into the site. It would also prevent them from exiting the site. Anti-passback is explained more in the StorLogix Operations Manual.

Bad Attempts Limit: This is used to help prevent code-hacking. If someone tries to guess codes by entering code after code, this can keep them from succeeding. A recommended setting for this is 3 - 5 attempts. That gives legitimate users the ability to make a mistake or two without getting locked out while interfering with someone attempting to guess codes. For example, if this is set to 3 attempts. After a potential thief enters three incorrect codes in a row, then on the fourth attempt, the keypad will prevent access (even for correct codes) for 60 seconds. Any key that the thief presses during that time will reset the 60 seconds. After the 60 seconds is up, the keypad returns to its normal state allowing new codes to be entered. Setting this to 0 turns off the function.

Click **Next** to Continue.

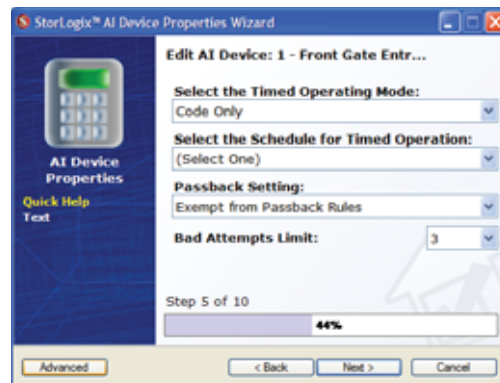


Figure 8-7 Setup AI Device Properties Wizard Advanced Step 5 of 10 - Select Timed Operating Mode, Passback Settings, and Bad Attempt Limits if Desired. Click Next to continue.

APPLICATION

Timed Operating Mode can be used to require users to use a code or card during business hours, but require the higher security card + pin function after business hours. Just setup the keypad or wiegand to be card+pin operating mode in Step 3 of the AI Device properties and setup the Timed operating mode as Code only during the time schedule that corresponds with the business hours.

CAUTION

Anti-passback functions are meant for higher security locations where employees and users can be well trained to use their access cards correctly and not tailgate. High security sites with guard booths and/or an active security team will find this to be a very helpful function.

Sites with high user turn-over like many self storage have with their customers will find this function to be frustrating as customers will often tailgate onto the site or off and get stuck when they try to come back.

Select the Alarm Zones for the AI Device. These can be the default Global Alarm Area that will sound an alarm throughout the site if one of these events happens, or it can sound only in the zone that the device is in, if the Alarm Zones have been setup that way in Chapter 5. Click **Next** to continue.

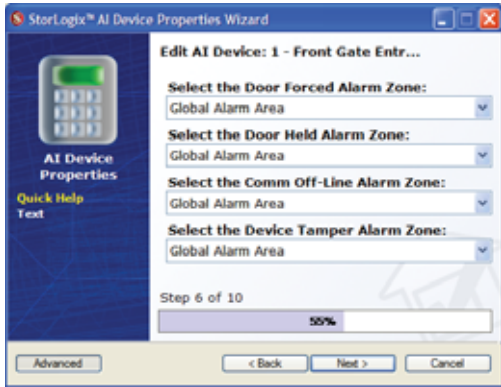


Figure 8-8 Setup AI Device Properties Wizard Advanced Step 6 of 10 - Select the Alarm Zones for each of these alarm event types.

Select the Power Fail alarm zone. Then select the Data Format for the wiegand device if one is connected to this AI Device. The data format will be in the manufacturers instructions.

Select a Valid Access message if custom messages are being used. If this is the first time the system is being setup, then there will not be any custom messages yet. Once they are entered, return to this step and select the message to display on a valid access.

Allow User Custom Messages should be checked if custom messages are being used at the site. Check-in Required is only used if there is a Check-in pad that must be activated before coming to this device. If the keypad IS the check-in device, do NOT check this box. Used for PayXpress is checked if the site is using PayXpress AND this device is one that customers can use for PayXpress functions.

Click **Next** to continue.



Figure 8-9 Setup AI Device Properties Wizard Advanced Step 7 of 10 - select the advanced options and click Next to continue.

???????? HINT

Alarm Zones and AI Devices

Door Forced Open: The door must have a door switch on it for this function to work. If it does and the door is opened without entering a valid code at the keypad, this alarm will sound.

Door Held: If the door has a door switch on it, this can be set in Step 9 of the Advanced settings. If the door is held open longer than the timer, then an alarm sounds.

Comm Off-Line: This alarm sounds if the AI Device loses communication with the Falcon XT.

Device Tamper: This alarm sounds if the AI Device is opened.

Power Fail: This alarm sounds if the AI Device loses power.

APPLICATION

When using PayXpress at a site, generally, only the entrance keypad to the site or a special keypad near the office is used for PayXpress and the PayXpress function is turned off at any other keypads on any other buildings. Otherwise, the client who elects not to pay his bill at the entrance (but is not overdue and locked out), will see the message at every keypad.

APPLICATION

Tripping relay(s) when an invalid attempt is made could be used to trigger a relay that lights a warning light on a board in the office.

Use it with Wiegand readers to control the color of the light or number of beeps on denied access.

It could also be used with a virtual relay and LogixScript counter to trigger an alarm after a certain number of invalid attempts.

REMEMBER

Door Held settings allow an alarm to be triggered if the door has an alarm switch on it and a user props the door open or holds it open for an extended period of time. The system can monitor up to two contacts per keypad. In most situations it will only have one contact for the door, however, some double door situations will have two contacts.

The Door Held Open Timeout is the length of time in hours, minutes, and seconds that the door can be held open before an alarm is registered.

APPLICATION

Request to Exit is used primarily when a single keypad controls a door. The user enters their code to go through the door. When they are ready to leave, they press a button, cross in front of a beam or motion sensor, or step on a pad that allows them to exit. This allows the door to be alarmed and the activity to be monitored, which cannot be done if the door just allows free exit with a knob or crashbar.

Select the relay(s) to trip with an invalid access attempt and click **Add**. Generally, this will not need to be set. See the Application note in the sidebar. Click **Next** to continue.

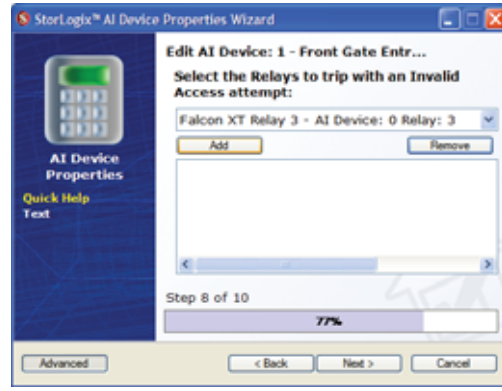


Figure 8-10 Setup AI Device Properties Wizard Advanced Step 8 of 10 - Select a relay to trip on an Invalid Access Attempt.

If the door is being used with Request to Exit function, select the door contacts for Held Open reporting as well as the Door Held Open Timeout. Click **Next** to continue.



Figure 8-11 Setup AI Device Properties Wizard Advanced Step 9 of 10 - Select the Request to Exit Door settings. Click Next.

Select the Request to Exit Input(s) if applicable. See Application note in sidebar for more information. Click **Done** to complete the process.



Figure 8-12 Setup AI Device Properties Wizard Advanced Step 10 of 10 - Select the Request to Exit Door Inputs. Then click Done.



Setup Falcon XT

The Falcon XT is the hardware controller that is operated using StorLogix.

Go to the Setup Screen in StorLogix. For more information on the Setup Screen, refer to the Setup Screen section in Chapter 3. Click on **17. Falcon XT**.



Figure 8-13 Setup Screen - Select 17. Falcon XT.

The Site Name is used to identify the Falcon XT when multiple Falcon XT's are connected to the same StorLogix. It is also the Site Name that will appear with custom messages.

The Aux Sirens are the auxiliary siren relays connected to PTI Hardwired Door Alarm Multiplexers and the buzzer alarms in Apex Keypads, VP Keypads, and RX-900 Wireless Door Alarm Multiplexers.

Log Off Time of Day clears all users off-site at the time set (usually sometime in the middle of the night). This clears off users who have tailgated off the site, rearming their doors and turning off any lighting zones or elevator activations.

Click **Next** to continue.



Figure 8-14 Setup Falcon XT Wizard Step 1 of 2 - Change the Site Name and Baud Rates if needed. Set the Global Siren Alarm Zone and Log Off Time of Day as necessary.

CAUTION

Generally, a site should NOT change the AI Devices Baud Rate or Host Baud Rate on this screen unless directed to do so by PTI Technical Support personnel for troubleshooting purposes.

CAUTION

Log Off Time of Day should be set to "None" on any site where there is 24 hour access to prevent users who are actually on-site from being cleared off-site and having alarms sound and the lights go off.

APPLICATION

Log Off Time of Day could be used to remove any users that may have tailgated off the site in a site with an entry and exit gate.

It could also be used in a building situation where everyone gets free exit without having to log off. This function then logs them off the site after hours to clear the lighting areas and elevator zones as well as turn all alarms back on.

Undefined Event Reporting is used primarily with the Wireless RX-900 system to make sure that all wireless devices are reporting in and defined in the system. Once the site has been completely installed and checked, these can be turned off.

The Use Facility Code option is for Proximity Cards. Generally, this will be left on. In some cases, when converting an older proximity card system to the StorLogix, the site may not be using the facility code and will need to turn this off.

The Entire Alarm System can be turned off here as well as Vacant Alarms and Communications Alarms. Vacant Alarms are the alarm events from unrented units. Communications Alarms happen when an AI Device is damaged or removed and can no longer communicate with the Falcon XT.

Allow Exit with Door Open is used only with Check In devices. If it is turned on, it will prevent a client from checking out if their door is opened. This function will not actually prevent the user from leaving the site, only from checking out. Click **Done** when complete.

HINT

It is a good idea to leave Vacant Alarms turned on. This can help prevent common self storage crimes such as illegal dumping, homeless squatting or drug trafficking and production in unrented units.



Figure 8-15 Setup Falcon XT Wizard Step 2 of 2 - Select the options and click Done.

A dialog box will appear. Click on the **Yes** button to save the settings.

Another dialog box will then appear to confirm that the Falcon XT changes were successfully saved. Click **Yes** to continue adding and editing the Falcon XTs, click **No** to return to the Setup Screen.



Figure 8-16 Setup Falcon XT Wizard confirmation dialog boxes

Setup Falcon XT - Advanced

The Falcon XT has advanced features that can be setup.

If the StorLogix Preferences were setup with 'Advanced Menus Always On', then the advanced steps will already be visible. If not, from Step 2 of the Falcon XT setup process, click on the **Advanced** button at the bottom left corner of the field. This adds advanced Steps 3 - 5. Click the **Next** button from Step 2 to get to this Advanced screen.

Poll Timeout (Milliseconds): The Falcon XT constantly polls the AI Devices to see if they have any information (such as requests for entry). This occurs many times each second. The Poll Timeout is the amount of time that the Falcon XT will wait for an answer from the device before recognizing that there is a communication error and moving on to poll the next device. This number should be set between 10 - 30 on most systems. On systems using Wireless RS485, the Poll Timeout should be set higher to 150 - 200.

Maximum AI Devices: Set this to the same number as the highest AI Device ID (address). It is the highest AI Device ID that the Falcon XT will look for while polling AI Devices.

Comm Count: This is the number of communication errors that the Falcon XT will ignore before reporting a Communications Off event. This can be turned down during troubleshooting for communications errors, but generally this should be set at 10. It is not a good idea to turn this number up any higher.

Maximum Code Size: This is used when the site uses magnetic swipe or proximity cards for access control. The Falcon XT automatically converts the code on the card to a 10 digit number for access. Some management software programs have a code length limit. If the Falcon XT is interfaced to one of these programs, the code size can be turned down to the required length for that software. Check with the management software manufacturer for their limitations. This is not an issue with TaskMaster as codes can be any length up to 10 digits.

Contrast Code: This is only used when the Falcon XT is connected to previous PTI keypad models manufactured before 2000, that did not have a backlit display, so the contrast had to be adjusted for lighting conditions. This contrast code could be entered on the keypad allowing the operator to press * to darken the screen or # to lighten. If the keypads are manufactured after the year 2000, this is not an issue as the displays are backlit. The Contrast Code can NEVER be used as an access code.

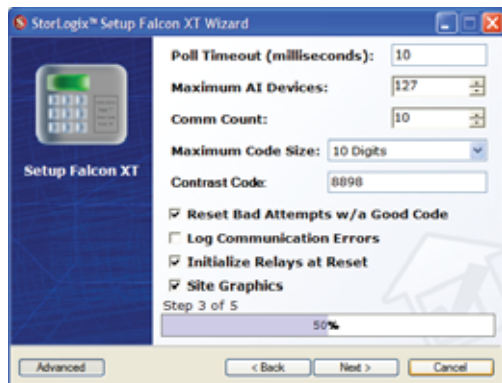


Figure 8-17 Setup Falcon XT Wizard Advanced Step 3 of 5 - Set the Poll Timeout, Maximum AI Devices, Comm Count, Maximum Code Size and Contrast code.

Reset Bad Attempts w/a Good Code: If the Bad Attempts function is being used with AI Devices (See Setup AI Devices advanced step 5 of 10 earlier in this chapter), then this allows the entry of a good access code to reset the bad attempts counter. For example, if the bad attempts is set at 3 and a client enters their code wrong 3 times in a row, then normally the system will lockout use of the keypad for 60 seconds and any code (good or bad) will reset the 60 second timer. If Reset Bad Attempts w/a Good Code is checked here, and the customer finally remembers their code and enters it correctly, then the good code will allow entry even during the lockout time. A bad code will still reset the 60 second timer..

Log Communications Errors: This function should be left unchecked by the user. It should only be activated if a PTI Technical Support technician instructs the site to do so during troubleshooting.

Initialize Relays at Reset: StorLogix must initialize all relays at least once before it can recognize their state (open or closed). This box is checkmarked by default. This allows the Falcon XT to set all relays to their correct state any time the Falcon XT is reset. Caution: If the this box is reset and the Falcon XT is reset, then every relay on the site will momentarily trigger, opening all relay controlled doors and gates and turning on any relay controlled lights and elevator buttons. PTI recommends that this function be checkmarked, but be aware of the momentary relay trigger of a system reset.

Site Graphics: Check this box if the site is using PTI Site Graphics.

When all options are selected, click **Next** to continue.



Figure 8-18 Setup Falcon XT Wizard Advanced Step 3 of 5 continued - Select the remaining options and click Next to continue.

Step 4 of 5 contains the communications settings for StorLogix. Do not make any changes to this screen unless instructed to do so by a PTI Technical Support technician. Generally, this screen should be skipped. Click **Next** to continue.



Figure 8-19 Setup Falcon XT Wizard Advanced Step 4 of 5 - Click Next to continue.

Select the Anti-passback mode. See the note in the sidebar.

Timed Anti-Passback: This is usually used in a mangate or turnstyle situation to prevent a user from handing their card back to another person to use. It is a set amount of time during which a user cannot enter the same area without actually exiting the area first. Set the time limit in the Anti-passback Time (minutes field below).

Logical Anti-Passback: This helps to control access with anti-passback. If this is set, a user cannot gain access to an area if they aren't already in the area before it. For example. If a site has an access controlled building on it as well as access control at the gate, a user can not use the keypad to access the building unless they first used the keypad to access the gate. This works off of the TO and FROM areas that are setup for each access device in the Setup AI Device Properties Function previously in this chapter.

Timed-Logical Anti-passback: This option combines both of the previous options into one.

Select the Late Exit mode. This controls user exit after the time schedule hours that they are allowed.

Free Late Exit: This is the option that most sites will use. Customers can freely enter and exit the site within their authorizations during their time schedule. After their time schedule is closed, they can still freely exit the site, but the exit will report in the event log as a late exit to allow tracking of this behavior.

No Late Exit: If this option is selected, Exit is limited only to Time Schedule hours. If the user's time schedule allows access from 8:00 am to 5:00 pm, they CANNOT exit the site after 5:00 pm. This is only for High Security Facilities and should NOT be used on most sites.

Timed Late Exit: This option gives the user a Grace Period set in the field immediately below the Late Exit Mode. Exit from the site is allowed during time schedule hours for the user. After the time schedule is closed, then the exit is allowed during a grace period, but will record a Late Exit event in the event log.

Counted Late Exit: Exit is allowed after time schedule hours, but the user is limited to the number of time that they can use this feature. Each time they exit after time schedule hours, it is counted and when it reaches the number set in the Late Exit Count Limit, they are suspended and must be reactivated by an administrator.

Timed - Counted Late Exit: This combines the above features of TImed and Counted, giving the user a grace period and only counting the late exit toward suspension if it is outside the grace period.

Select **Done** to complete this wizard.

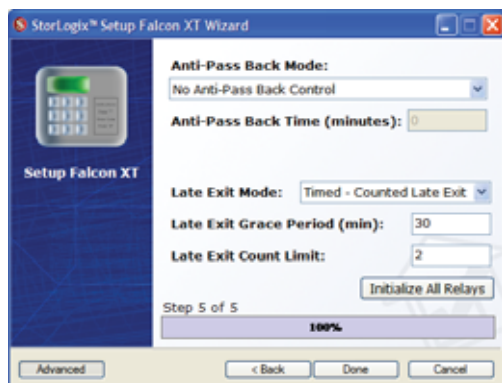


Figure 8-20 Setup Falcon XT Wizard Advanced Step 5 of 5 - Select the Anti-passback and Late Exit options. Then, click Next to continue.



REMEMBER

Anti-passback is used to prevent 'tailgating' where a user follows someone else onto the site or into an area without using their own code. It also helps prevent users from 'passing back' their card to another user who forgot their card. The ultimate goal is to keep track of who is actually on-site and prevent access to unauthorized persons.

Anti-passback functions are meant for higher security locations where employees and users can be well trained to use their access cards correctly and not tailgate. High security sites with guard booths and/or an active security team will find this to be a very helpful function.

Sites with high user turn-over like many self storage have with their customers will find this function to be frustrating as customers will often tailgate onto the site or off and get stuck when they try to come back.

Chapter Terms

AI Device	Any Keypad, Multiplexer, Relay Board, or Wiegand device. In previous Falcon Systems, this was referred to as a Remote.
AI Device ID	The unique identifier number programmed in to each AI Device to differentiate it from other AI Devices when communicating to the Falcon XT. Referred to as Address in previous Falcon Systems.
Anti-passback	Anti-passback is used to prevent 'tailgating' where a user follows someone else onto the site or into an area without using their own code. It also helps prevent users from 'passing back' their card to another user who forgot their card. The ultimate goal is to keep track of who is actually on-site and prevent access to unauthorized persons. Anti-passback functions are meant for higher security locations where employees and users can be well trained to use their access cards correctly and not tailgate. High security sites with guard booths and/or an active security team will find this to be a very helpful function. Sites with high user turn-over like many self storage have with their customers will find this function to be frustrating as customers will often tailgate onto the site or off and get stuck when they try to come back.
Bad Attempts Limit	This is used to help prevent code-hacking. If someone tries to guess codes by entering code after code, this can keep them from succeeding. A recommended setting for this is 3 - 5 attempts. That gives legitimate users the ability to make a mistake or two without getting locked out while interfering with someone attempting to guess codes. For example, if this is set to 3 attempts. After a potential thief enters three incorrect codes in a row, then on the fourth attempt, the keypad will prevent access (even for correct codes) for 60 seconds. Any key that the thief presses during that time will reset the 60 seconds. After the 60 seconds is up, the keypad returns to its normal state allowing new codes to be entered. Setting this to 0 turns off the function.
Card Only	For keypads with card readers, it lets the keypad accept access using just a card.
Card+Pin	For Apex keypads with card readers, this high security feature requires a card and a pin number to prevent stolen cards from gaining access.
Check In/Out	This function allows a keypad to be setup so that everyone must check-in at this location (such as in the office) before they can use any other keypad or open any alarmed door on the site. They must also check out at this keypad. Often this is used when the site is accessed through one main lobby with multiple wings and hallways that are access controlled beyond the lobby. A user must checkin at the lobby keypad before they can use any other keypad or alarmed door on the site.
Code Only	For keypads that do not have cards, this lets the keypad function by using the touchpad.
Comm Count	This is the number of communication errors that the Falcon XT will ignore before reporting a Communications Off event. This can be turned down during troubleshooting for communications errors, but generally this should be set at 10. It is not a good idea to turn this number up any higher.
Comm Off-Line	This is when an AI Device no longer is communicating with the Falcon XT.

Contrast Code	This is only used when the Falcon XT is connected to previous PTI keypad models manufactured before 2000, that did not have a backlit display, so the contrast had to be adjusted for lighting conditions. This contrast code could be entered on the keypad allowing the operator to press * to darken the screen or # to lighten. If the keypads are manufactured after the year 2000, this is not an issue as the displays are backlit. The Contrast Code can NEVER be used as an access code.
Counted Late Exit	Exit is allowed after time schedule hours, but the user is limited to the number of time that they can use this feature. Each time they exit after time schedule hours, it is counted and when it reaches the number set in the Late Exit Count Limit, they are suspended and must be reactivated by an administrator.
Data Format	For wiegand devices this is the specific protocol type for the device. There are many types of these. The PTI system is compatible with 26 bit, 30 bit, 31 bit, and 34 bit. Refer to the wiegand device manufacturer's instructions for the specific Data Format for the device.
Device Tamper	Tamper switches built into AI Devices. These always report as an alarm even if authorized users are logged into the area.
Door Forced Open	Doors that are directly controlled by keypads or wiegand devices for access can have door contact switches placed on them to activate alarms if the door is forced open without entering a valid code or card.
Door Held Open	Doors that are directly controlled by keypads or wiegand devices for access can have door contact switches placed on them to activate alarms if the door is held open longer than a preset amount of time.
Door Held Timeout	This is the length of time that an access controlled door with a door contact switch can be held open before the Door Held Open alarm is activated. See Door Held Open.
Entry/Exit	This is used primarily when there is only one keypad on a site with alarms. Users must come and enter their code at this keypad to turn off the alarm at their unit. The second time they enter their code at this device, it turns the alarm back on.
Facility Code (Prox Cards)	This is an extension of the Proximity Card code length in most types of proximity cards. Generally, this will be left on. In some cases, when converting an older proximity card system to the StorLogix, the site may not be using the facility code and will need to turn this off.
Free Late Exit	This is the option that most sites will use. Customers can freely enter and exit the site within their authorizations during their time schedule. After their time schedule is closed, they can still freely exit the site, but the exit will report in the event log as a late exit to allow tracking of this behavior.
From Access Area	The area outside an access controlled "To Access Area". For example, in most sites, the primary From Access Area will be called Offsite (everything outside the fence line). The primary To Access Area would be called On-site (everything inside the fence line). Other access controlled areas inside the site might be further To Access Areas. For example, an access controlled building inside the site would have a From Access Area of On-site and a To Access Area of Building A. Building A may have an access controlled Wine Storage inside it with a From Access Area of Building A to a To Access Area named Wine Storage. See From Access Area.
Input	A point in the system that alarm switches, motion sensors, glass break sensors, door contacts, or tamper switches can be connected.

Invalid Access Attempt	When someone enters a code or presents a card at a keypad or wiegand device that is not allowed access due to an incorrect code entry, being outside of their time schedule, trying to enter an access area that they are not authorized for, or trying to enter when they are suspended. The keypad or wiegand device will deny access. See also Valid Access Attempt.
Late Exit	Exit after the time schedule assigned to the user.
Log Off Time of Day	Optional setting that clears all users off the site at a certain time every day to remove users that may have tailgated off the site from the access. This should not be used on-sites with 24 hour access.
Logical Anti-Passback	This helps to control access with anti-passback. If this is set, a user cannot gain access to an area if they aren't already in the area before it. For example, if a site has an access controlled building on it as well as access control at the gate, a user can not use the keypad to access the building unless they first used the keypad to access the gate. This works off of the TO and FROM areas that are setup for each access device in the Setup AI Device Properties Function previously in this chapter.
Maximum AI Devices	Set this to the same number as the highest AI Device ID (address). It is the highest AI Device ID that the Falcon XT will look for while polling AI Devices.
Maximum Code Size	This is used when the site uses magnetic swipe or proximity cards for access control. The Falcon XT automatically converts the code on the card to a 10 digit number for access. Some management software programs have a code length limit. If the Falcon XT is interfaced to one of these programs, the code size can be turned down to the required length for that software. Check with the management software manufacturer for their limitations. This is not an issue with TaskMaster as codes can be any length up to 10 digits.
No Late Exit	Exit is limited only to Time Schedule hours. If the user's time schedule allows access from 8:00 am to 5:00 pm, they CANNOT exit the site after 5:00 pm. This is only for High Security Facilities and should NOT be used on most sites.
Passback Setting	This setting in the Setup AI Device Properties wizard allows each keypad or wiegand access device to be setup with specific properties of the Anti-passback settings or to be exempt from the site Anti-passback rules. See Anti-passback for more information.
PayXpress	Module in TaskMaster and StorLogix that allows credit card payments to be made from an APEX keypad so customers can pay at the gate.
Poll Timeout	The Falcon XT constantly polls the AI Devices to see if they have any information (such as requests for entry). This occurs many times each second. The Poll Timeout is the amount of time that the Falcon XT will wait for an answer from the device before recognizing that there is a communication error and moving on to poll the next device. This number should be set between 10 - 30 on most systems. On systems using Wireless RS485, the Poll Timeout should be set higher to 150 - 200.
Power Fail	This is an alarm event that occurs when the Falcon XT device loses power and is running off of its battery power.
Relay	A switch located in electronics used to control another device. May be physical or virtual. See Also Physical Relay and Virtual Relay.

Request to Exit Inputs	These are inputs in the system that are used for exit on Access Controlled Doors so that there doesn't have to be a keypad on both sides of the door. A push button is generally wired into an input in the keypad or the Falcon XT and it is then designated as a request to exit input for that door in StorLogix. When a user pushes that button, it will trigger the relay allowing the user to exit the door without setting off the Door Forced Open alarm.
Timed - Counted Late Exit	This combines the features of Timed and Counted Late Exit, giving the user a grace period and only counting the late exit toward suspension if it is outside the grace period.
Timed - Logical Anti-passback	This option combines Timed Anti-passback and Logical Anti-passback, so a user cannot enter an area if they were not already in the logical area outside the one they want to enter and they cannot re-enter that area again within the timed setting unless they first exit it. See Timed Anti-Passback and Logical Anti-passback.
Timed Anti-Passback	This is usually used in a mangate or turnstyle situation to prevent a user from handing their card back to another person to use. It is a set amount of time during which a user cannot enter the same area without actually exiting the area first. Set the time limit in the Anti-passback Time (minutes field below).
Timed Late Exit	This option gives the user a Grace Period set in the field immediately below the Late Exit Mode. Exit from the site is allowed during time schedule hours for the user. After the time schedule is closed, then the exit is allowed during a grace period, but will record a Late Exit event in the event log.
Timed Operating Mode	Mode (code only, card only, or card+pin) that a keypad will operate with during a specific time schedule. Outside of that time schedule, it will operate in its assigned Operating Mode. Both Operating Mode and Timed Operating Mode are found in the Setup AI Device Properties wizard.
To Access Area	The area inside an access controlled fence line, building, or room. As you enter a code at a keypad or card at a reader, you cross from the "From Access Area" into the "To Access Area". For example, in most sites, the primary From Access Area will be called Offsite (everything outside the fence line). The primary To Access Area would be called On-site (everything inside the fence line). Other access controlled areas inside the site might be further To Access Areas. For example, an access controlled building inside the site would have a From Access Area of On-site and a To Access Area of Building A. Building A may have an access controlled Wine Storage inside it with a From Access Area of Building A to a To Access Area named Wine Storage. See From Access Area.
Valid Access Attempt	When a valid user enters their code or presents their card at a keypad or wiegand device, the system will trigger the relay to open the door or gate. See also Invalid Access Attempt.
Wiegand Device	An AI Device that communicates with Wiegand Protocol Devices such as proximity card readers, fingerprint readers, or key fobs.

CHAPTER 9: OPTIONAL SETUP

- **SETUP DVR**
- **SETUP HOLIDAYS**
- **SETUP EVENTS TO VIEW**

These items only need to be setup if the site will be using the functions. DVR (Digital Video Recorder) Integration is a module that is only compatible with certain DVR's purchased from PTI. Holidays are only used if the site has restricted hours or is completely closed on holidays. Events to View can be used to narrow the number and type of events that report to help smaller sites focus on the events that they want to watch specifically watch for.



Setup DVR

Integrating a DVR (Digital Video Recorder) with StorLogix allows events in the event log to be clicked on to show the video from that area at the time of the event, so that the site doesn't have to search through hours of video to find out what happened when an alarm occurred.

Go to the Setup Screen in Storlogix. For more information on the Setup screen, refer to the Setup Screen section in Chapter 3. Click on **18. DVR**.



Figure 9-1 Setup Screen - Select 18. DVR.

Select **Add** and click on **Next** to add a new DVR.

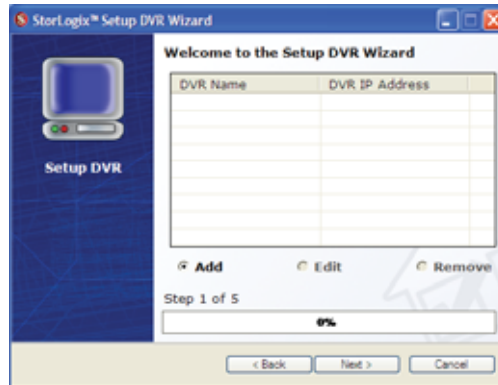
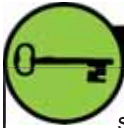


Figure 9-2 Setup DVR Wizard Step 1 of 5 - Select Add to add a DVR to the system. Click Next to continue.



????????? HINT

Multiple DVR's can be setup for the same site or for the same StorLogix system over multiple sites.

Large sites may require multiple DVR's to handle many cameras as most DVR's are limited to the number of cameras that they can be connected to (generally this is between 4 and 16 cameras).

Owners of multiple sites can have a DVR at each site that integrates with the StorLogix in the central office so that the owner is able to check on the video associated with specific events.

NOTE: Only PTI compatible DVR's can be integrated to StorLogix. Contact PTI for a current list of compatible DVR's.



APPLICATION

With a carefully planned security and video layout, the DVR Integration can greatly improve the security of the site.

Events can be integrated with the video by using the Inputs to Cameras, AI Devices to Cameras, and Relays to Cameras functions. This can help provide instant footage of crimes or identification photos of the criminal for the police without having to watch hours of video tape footage or try to figure out how to find the event in the DVR. Just click on the event and the footage appears.

Enter a description for the DVR. This is especially important if more than one DVR is used for the site. Then, enter the DVR IP Address and password. The IP Address is the network address for the DVR and can be obtained from the technician who setup the DVR along with the password.

Click **Next** to continue.

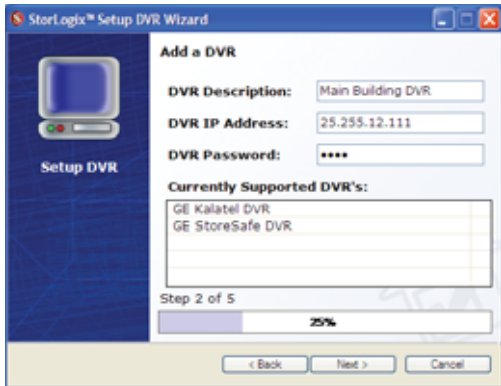


Figure 9-3 Setup DVR Wizard Step 2 of 5 - Enter the DVR Description, IP Address, and Password. Click Next to continue.

Select the specific inputs to associate with DVR cameras. Select an input and then select a camera to associate with it. Then click on the Add button. Continue this process until all inputs are associated with the nearest camera. Then, click **Next** to continue.

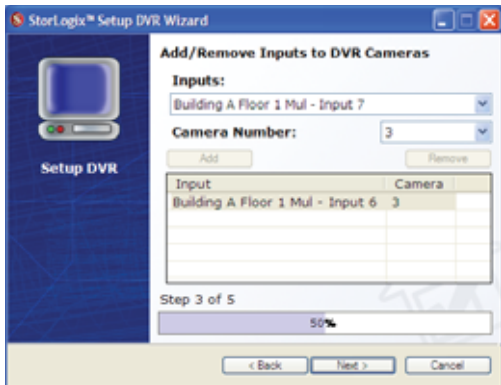
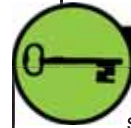


Figure 9-4 Setup DVR Wizard Step 3 of 5 - Select the inputs that are associated with each camera. Click Next to continue.



???????? HINT

See the Networking section in Chapter 10 for more information on DVR setups in a network situation.



APPLICATION

Inputs to Cameras

This useful function allows the site to associate alarm inputs to specific cameras.

For example, a site has camera # 1 aimed down a hallway with units 1 - 100 and these units have door alarms. Select each input for doors 1 - 100 and associate them with camera # 1 on this wizard. Then, if any events or alarms occur on these doors, the site manager can click on that event in the event log and see the video from camera # 1 at the time of the event, immediately, without having to review hours worth of footage.

Select each AI Device to associate with the nearest camera. Select the camera number and click on the **Add** button. When all AI Devices are associated as needed, click on the **Next** button.

APPLICATION
AI Devices to Cameras

This useful function allows individual AI Devices to be associated with the nearest camera.

For example, a site has a keypad on the back door to the building and a camera pointed at the keypad. Any activity, events, or alarms generated by that keypad will automatically be associated with that camera allowing the site manager to click on the event and immediately see camera footage from that event without having to search through hours of footage.

This is an especially handy function if used with pinhole cameras in the keypad. This allows you to get a picture of each person entering their code.

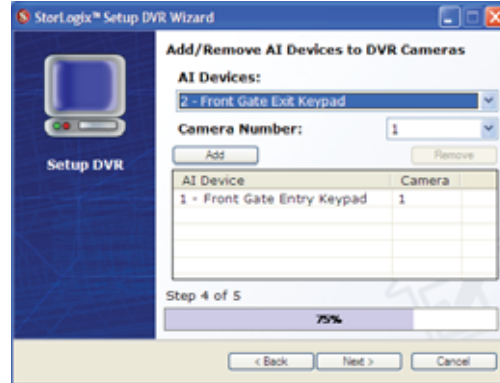


Figure 9-5 Setup DVR Wizard Step 4 of 5 - Select the AI Devices that are associated with each camera. Click Next to continue.

Select each relay to associate with the nearest camera. Select the camera number and click on the **Add** button. When all relays are associated as needed, click on the **Done** button.

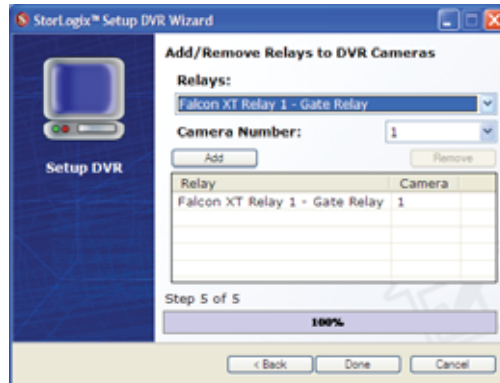


Figure 9-6 Setup DVR Wizard Step 5 of 5 - Select the Relays that are associated with each camera. Then click Done.

A dialog box will appear. Click on the **Yes** button to save the DVR.

Another dialog box will then appear to confirm that the DVR changes were successfully saved. Click **Yes** to continue adding and editing DVR's, click **No** to return to the Setup Screen.

APPLICATION
Relays to Cameras

This useful function allows individual Relays to be associated with the nearest camera.

For example, a site has an entrance and exit keypad on the main gate and a license plate camera pointed at the car. Anytime the gate relay is triggered to open the gate, it will automatically be associated with that camera allowing the site manager to click on the event and immediately see camera footage from that event without having to search through hours of footage.

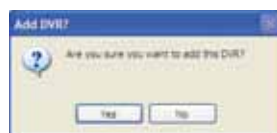


Figure 9-7 Setup DVR Wizard confirmation dialog boxes.





Setup Holidays

Holidays in StorLogix are only used if the site has different hours for a certain day or is closed on that day. Holidays must be updated each year.

Go to the Setup Screen in Storlogix. For more information on the Setup screen, refer to the Setup Screen section in Chapter 3. Click on **19. Holidays**.



Figure 9-8 Setup Screen - Select 19. Holidays.

Click on Add and then the Next button to input a holiday.



Figure 9-9 Setup Holidays Wizard Step 1 of 3 - Select Add to add a Holiday to the system. Click Next to continue.

Enter the holiday description, start and end date/time. Then click **Next**.

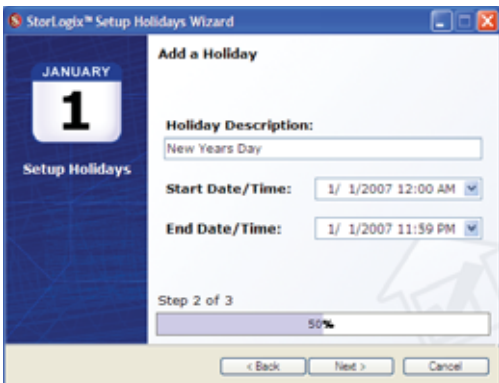


Figure 9-10 Setup Holidays Wizard Step 2 of 3 - Enter the holiday description and the start and end time for the holiday. This is the time that the system will switch from regular time schedule hours for that day of the week to holiday hours.

REMEMBER

Holidays do not have to be input in StorLogix unless the site actually has different hours or is closed for that day. Holidays are specific to each time schedule so it is possible to have shortened hours for customer while still allowing employees access.

CAUTION

The Start & End Date/Time is NOT the actual hours that access is allowed for that day. It is the time during which StorLogix will switch from the regular time schedule hours for that day of the week to the holiday time schedule hours. This is setup individually in each time schedule. Refer to the Setup Time Schedules Section in Section 3 for more information on this.

Select a time schedule that this holiday applies to and click the **Add** button. If a time schedule is not affected by the holiday (such as for employees who will be working that day), it does not need to be selected (or the holiday hours in the Setup Time Schedules wizard can be set as the same as normal weekday hours).

Click **Done** when finished.

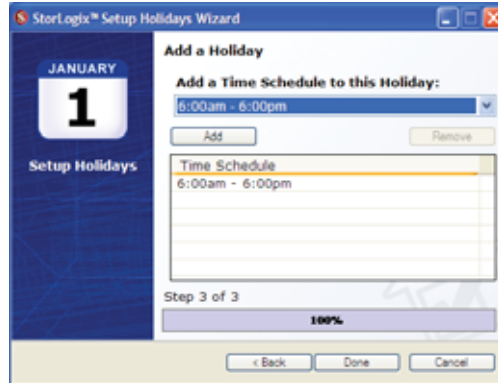


Figure 9-11 Setup Holidays Wizard Step 2 of 3 - Enter the holiday description and the start and end time for the holiday. This is the time that the system will switch from regular time schedule hours for that day of the week to holiday hours.

A dialog box will appear. Click on the **Yes** button to save the Holiday.

Another dialog box will then appear to confirm that the Holiday was successfully saved. Click **Yes** to continue adding and editing Holidays, click **No** to return to the Setup Screen.



Figure 9-12 Setup Holidays Wizard confirmation dialog boxes



Setup Events to View

StorLogix has over 650 possible events that are reported by the system. This wizard allows the site to customize which events that they want to see as well as create alert emails or sounds that happen with certain events.

Go to the Setup Screen in Storlogix. For more information on the Setup screen, refer to the Setup Screen section in Chapter 3. Click on **20. Events to View**.



Figure 9-13 Setup Screen - Select 20. Events to View.

Select an event from the list and click on **Next**.

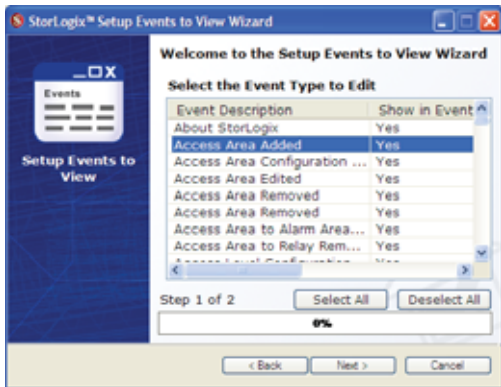


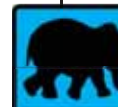
Figure 9-14 Setup Events to View Wizard Step 1 of 2 - Select an Event or Events from the list. Click Next to continue.



???????? HINT

Many of these events are useful for day-to-day site operations. Many are only useful for troubleshooting or audit trail investigation. This wizard allows the site to select only those events that they want to see and hide those that they do not want to see.

Even if events are hidden, they are still recorded and can always be viewed later if necessary.



REMEMBER

Multiple events can be selected at once by using the shift key to select a group or the control key to select multiple individual events.

This allows multiple events to be shown or hidden without having to go to each event individually.

Select whether to show the event in the Event Log and Site Graphics.

Email Alerts can be sent with certain events. Refer to the Setup Alerts section in the next chapter for more information on Alerts.

Events can also make a sound on the computer when they occur to help the manager know when an event is occurring. These .wav sound files can be found in the Sounds folder in StorLogix.

Click **Done** when this screen is completed.

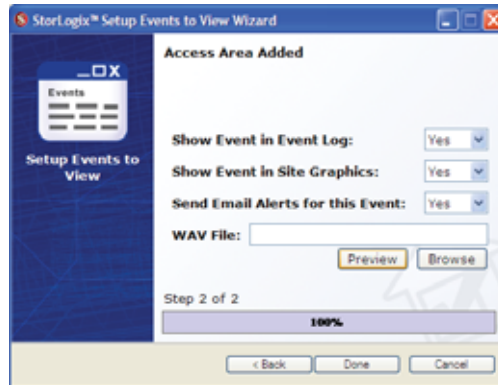


Figure 9-15 Setup Events to View Wizard Step 2 of 2 - Select the desired options for the event and then click Done.

A dialog box will appear. Click on the **Yes** button to save the Holiday.

Another dialog box will then appear to confirm that the Holiday was successfully saved. Click **Yes** to continue adding and editing Holidays, click **No** to return to the Setup Screen.

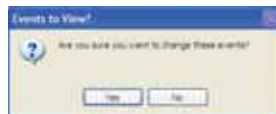


Figure 9-15 Setup Events to View Wizard confirmation dialog boxes.



REMEMBER

Even if events are not shown in the Event Log or Site Graphics, they are still kept in the database and can be viewed at a later date if needed.

APPLICATION

Email Alerts can be setup so that certain events will trigger an email to be sent.

This could be used for managers or security guards to receive emails on the computer, email pager, or cell phone when an alarm goes off at the site.

Alerts can be customized in many ways. Refer to the Setup Alerts section in the next

HINT

There are over 600 possible events in StorLogix. A complete list of these events and their meanings is available in the Help section of the StorLogix program.

Chapter Terms

AI Devices to Camera	To associate an AI Device to a specific camera to allow any events from that device to show the video from that camera at that time when the event is clicked on.
Alerts	Emails that StorLogix can send based on events. See Chapter 10.
DVR	Digital Video Recorder.
DVR IP Address	A unique identifier number assigned to Digital Video Recorder computers on a network to differentiate them from each other computers or DVR's.
Event	Occurrences and actions within StorLogix that are recorded and may appear on the event log. For example, when a user presents their card for valid access at a gate, at least four events will occur: "Known Card Presented", "Access Granted", "Relay Activated", and "Relay Deactivated". Each of these 'events' will appear as a line item on the Event Log (if selected to show within Events to View).
Events to View	A setup wizard in the setup screen that allows events to be shown or not shown on the event log. Not showing them does not delete the event; the event still is there and can be reviewed later if necessary. This wizard also allows sounds and alerts to be associated with each event.
Holiday	A program setting in StorLogix that allows the regular access hours to change or be locked out on certain days of the year.
Holiday End Time	The actual time during the day on a holiday date when the Holiday hours end. This allows regular access to resume after this time.
Holiday Start Time	The actual time during the day on a holiday date when the Holiday hours begin. Regular access hours are active until this time.
Inputs to Camera	To associate an input to a specific camera to allow any events from that input to show the video from that camera at that time when the event is clicked on.
IP Address	A unique identifier number assigned to computers on a network to differentiate them from each other.
Relays to Camera	To associate a relay to a specific camera to allow any events from that relay to show the video from that camera at that time when the event is clicked on.
Time Schedule	Preset timetables used for access permission and scheduled functions in StorLogix.
WAV file (.wav)	.wav sound files are a type of sound file that can be used in connection with StorLogix events so that when the event occurs, the sound plays on the computer to get the operator's attention. This is setup in the Setup Events to View wizard in Chapter 9.

CHAPTER 10: OTHER SETUP

- **CARDS**
- **CUSTOM MESSAGES**
- **CUSTOM MESSAGES ASSIGNED TO USERS**
- **CUSTOM MESSAGES ASSIGNED TO DEVICES**
- **ALERTS**
- **INPUTS TO RELAYS**
- **NETWORKS**
- **INTERFACE TO TASKMASTER**
- **INTERFACE TO OTHER MANAGEMENT SOFTWARES**

This section includes many optional setup items that are not listed on the main setup screen. None of these items are required for StorLogix to work at a site, but still may commonly be used.



Setup Cards

To use swipe cards or proximity cards with keypads, the cards must first be entered into StorLogix. They are saved in the system and selected from a list as units are rented to users or as users are added to the system.

Click on Edit on the menu bar. Highlight card in the drop down menu and then select **Setup Cards**.



Figure 10-1 Setup Screen - From the Menu Bar, select Edit. From the drop down menu, select Cards and then Setup Cards.

To enroll new cards, click on **Add** and then the **Next** button.



Figure 10-2 Setup Cards Wizard Step 1 of 2 - To Add card(s), click Add then Next.

APPLICATION

Sites that do not use cards can still use this function to store a preset list of site approved access codes that can be punched into keypads.

HINT

Setup the cards as soon as they are received so that if there is a lost card or stolen card, the system will recognize it as a card belonging to the site and warn the site operator that someone attempted to make entry to the site with a known card that wasn't assigned to anyone.

To add a single card, type the **Code** in the first field. The **To** field will reflect the same code. To add a range of cards, type the lowest card number in the **Code** field and the highest number in the **To** field.

Cards can be given a **Name** and **Description** if entered individually. Ranges of cards do not allow this.

Cards can also limited to a certain **Number of Uses Allowed** or to a certain time period by setting the **Start Date** and **End Date**.

If a card is lost or stolen, return to this screen and edit the card. Click in the **Lost** checkbox at the top of the window. This will allow StorLogix to recognize the card as lost so that anyone trying to use the card will be prevented access and the system will show that someone attempted to use a lost or stolen card.

Click **Done** when finished.

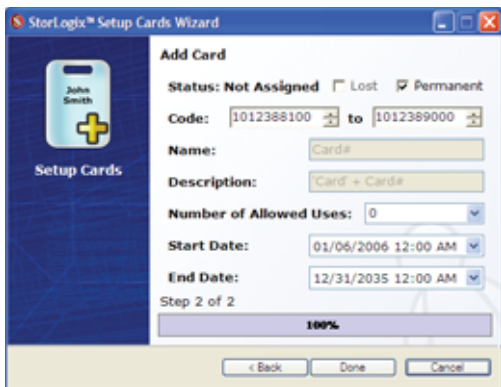


Figure 10-3 Setup Cards Wizard Step 2 of 2 - Select the options and enter the codes. Click Done.

A dialog box will appear. Click on the **Yes** button to save the Card(s).

Another dialog box will then appear to confirm that the cards were successfully saved. Click **Yes** to continue adding and editing cards, click **No** to return to the Setup Screen.



Figure 10-4 Setup Cards Wizard confirmation dialog boxes

??????? HINT

If the site intends to continue using the same cards again and again, requiring users to return them after they leave the company or quit renting from the site, click the **Permanent** checkbox at the top of the window. This will return the card number to the available list after a user is made inactive. If this is not checked, then the card will be removed from the system at the same time as the user.

Once the cards are entered, they can be edited individually or in groups. Select a card from the list on Step 1 of 2.

Multiple cards in a range can be selected by holding down the shift key while selecting the first and last card in the range. All of the cards between will be selected too. Holding down the Control (CTRL) key while selecting multiple cards allows selection of multiple cards that are not in a range. This allows only the cards clicked on to be selected.

Select card(s) and click on **Edit**. Then click **Next**.

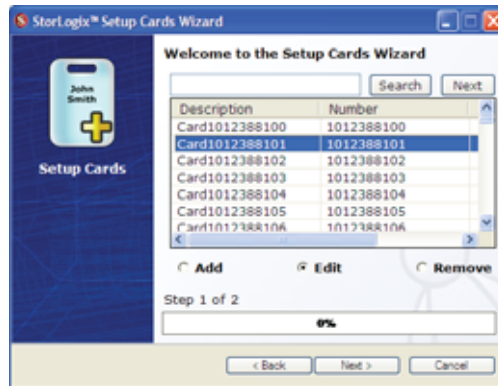


Figure 10-5 Setup Cards Wizard Step 1 of 2 - To Edit card(s), click Edit then Next.

When editing an individual card, the wizard Step 2 of 2 will show the number of times that the card has been used at the top of the window. This can be used by the site to count the number of uses. This number can be reset to zero by clicking on the **Reset** button next to it.

Make any changes to the screen and click the Done button. Any changes made will affect all of the cards selected in the previous step.

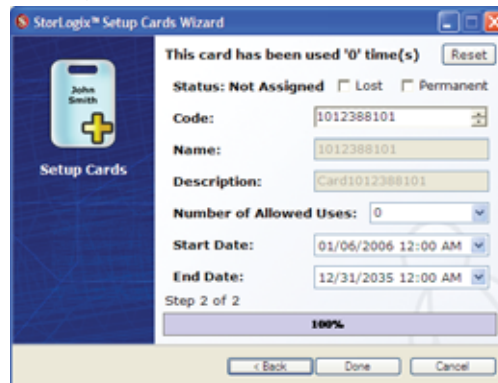


Figure 10-6 Setup Cards Wizard Step 2 of 2 - Edit the card(s), then click Done.

Setup Custom Messages



Custom Messages are a key feature of StorLogix. These are the messages that appear on the keypad displays when a user enters a code.

There are two types of custom messages: Default Messages and User Custom Message. Default Messages are the existing system messages such as “Welcome, Entry is Granted.” These can be changed to more personal greeting such as “Mr. Jones, Welcome to Smith Enterprises, please come in”

User Custom Messages are message that can appear for specific individual users, groups of users, or all users. These could be advertisements and reminders such as “We sell Boxes” or “Don’t forget to lock your door”. They could also be specific messages such as “Please come to the office to pickup a package” or “Mr. Jones, there is a message for you, see the manager.”

Click on Edit on the menu bar and select **Setup Custom Messages**.



Figure 10-7 Setup Screen - From the Menu Bar, select Edit. From the drop down menu, select Custom Messages.

To edit Default Messages, click on **Edit a Default Message** and then click the **Next** button.

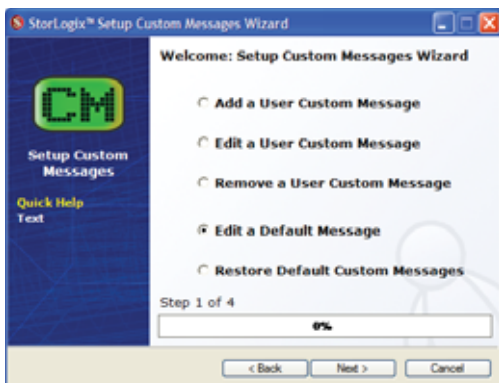


Figure 10-8 Setup Custom Messages Wizard Step 1 of 4 - To Edit Default Message(s), click Edit a Default Message, then Next.

Select the Default Message to Edit from the list. Default Messages do not allow a different **Message to Use Next** or **Repeat this Message (times)**.

Delay Before Activating Relay (s) is the amount of time between the message being displayed and the relay tripping to open the gate or door AND on Apex keypads only, it is the amount of time in seconds that the message is displayed for.

Flash Display causes the message to flash on and off the display during the **Delay Before Activating Relay (s)** amount of time.

Beep when Displayed causes the keypad to beep times in succession when the message is displayed. This can be used to get the customer's attention to read the message.

Click **Next** to continue.



Figure 10-9 Setup Custom Messages Wizard Step 2 of 4 - Select the message to edit, set the delay, repeat, flash, and beep functions. Then click Next.

Enter the message that should appear on 4x20 displays such as the Apex series keypads. Messages can be Right or Left justified or centered using the buttons to the right of each line. The message appears on the sample screen as it will appear on the Apex. Click **Next** to continue.



Figure 10-10 Setup Custom Messages Wizard Step 3 of 4 - Enter the text as the message will appear on an Apex keypad. Then click Next.

CAUTION

Be careful when setting the **Delay Before Activating Relay (s)** field. This is also the time the user will have to wait for the relay to trip to open the gate or door. Generally, this shouldn't be set for more than about 3 - 7 seconds. Any more than this can be annoying.

APPLICATION

Several system fields can be displayed as part of the custom message by inputting certain codes below.

Code	Displays
[D	Date Format mm/dd/yy
[d	Date Format dd/mm/yy
[S	Site Name
[T	Time hh:mm:ss am/pm
[t	Time hh:mm 24 hour
[U	The User 'display' name

Enter the message that should appear on 2x16 displays such as the VP series keypads. Messages can be Right or Left justified or centered using the buttons to the right of each line. The message appears on the sample screen as it will appear on the keypad. Click **Done** to continue.



Figure 10-11 Setup Custom Messages Wizard Step 4 of 4 - Enter the text as the message will appear on an VP keypad. Then click Done.

Another dialog box will then appear to confirm that the message was successfully saved. Click **OK**.



Figure 10-12 Setup Custom Messages Wizard confirmation dialog box.

Default Custom Messages can be restored back to the original messages at any time by clicking on **Restore Default Custom Messages** in Step 1 and clicking on **Done**.



Figure 10-13 Setup Custom Messages Wizard Step 3 of 4 - Restoring Default Custom Messages.

?
HINT

Keypad Displays are limited to the number of lines and characters that they will display.

VP Series Keypads have 2 x 16 displays that show 2 lines of 16 characters each.

Apex Series Keypads have 4 x 20 displays that show 4 lines of 20 characters each.

Long site names or user names may run off the edge of the display if using the system field codes and the information is more than 16 or 20 characters (VP or Apex series).

To edit User Custom Messages, begin from the same Step 1 of the Setup Custom Messages Wizard and click on **Add a User Custom Message**. Then click the **Next** button.



Figure 10-14 Setup Custom Messages Wizard Step 1 of 5 - Add User Custom Messages.

Enter the Message Description. This is the name of the message that allows it to be chosen from lists later.

Then select the **Message to Use Next** if applicable. See the Application note in the sidebar for more information on this.

Delay Before Activating Relay (s) is the amount of time between the message being displayed and the relay tripping to open the gate.

Repeat this Message will cause the message to appear for a user this number of times, after which they will see the regular access message.

Flash Display causes the message to flash on and off the display during the **Delay Before Activating Relay (s)** amount of time.

Beep when Displayed causes the keypad to beep times in succession when the message is displayed.

Click **Next** to continue.

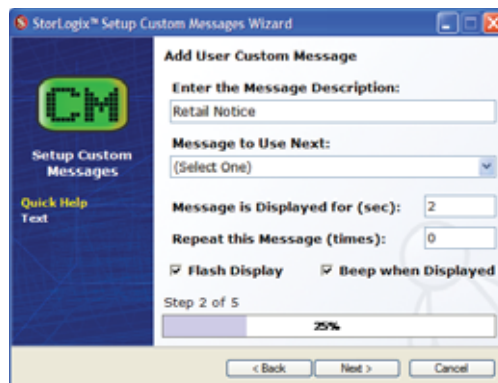


Figure 10-15 Setup Custom Messages Wizard Step 2 of 5 - Enter the User Custom Message description, the message to use next, and the display properties for the message.

APPLICATION

Message to Use Next:

Example:

A site has 3 messages that it wants clients to see: "We sell boxes", "Refer a friend for a discount", and "Don't forget to lock your door". Each message must be created separately.

When Message 1 "We sell boxes" is setup, the Message to use Next would be Message 2 "Refer a Friend".

When Message 2 is setup, the message to use next would be Message 3 "Don't forget to lock your door."

When Message 3 is setup, the message to use next would be Message 1 to start the cycle over again.

Each time the user enters their code at a keypad, they will see a different custom message.

Enter the message that should appear on 4x20 displays such as the Apex series keypads. Messages can be Right or Left justified or centered using the buttons to the right of each line. The message appears on the sample screen as it will appear on the Apex. Click **Next** to continue.



Figure 10-16 Setup Custom Messages Wizard Step 3 of 5 - Enter the text as the message will appear on an Apex keypad. Then click Next.

Enter the message that should appear on 2x16 displays such as the VP series keypads. Messages can be Right or Left justified or centered using the buttons to the right of each line. The message appears on the sample screen as it will appear on the keypad. Click **Next** to continue.



Figure 10-17 Setup Custom Messages Wizard Step 4 of 5 - Enter the text as the message will appear on a VP keypad. Then click Next.

Select the users who will see the message and then click **Done**.

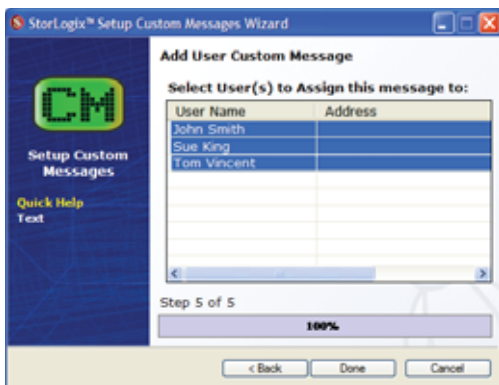


Figure 10-18 Setup Custom Messages Wizard Step 5 of 5 - Select the users that will see the message. Then click Done.

Custom Messages Assigned to Users

Custom Messages can be assigned to individual users. Click on the Edit User icon on the main StorLogix Screen.



Figure 10-19 StorLogix Main Screen - Select Edit User to add a custom message to a user.

Select a user to edit from the list and click **Next**. Keep clicking Next until Step 4 of 8 appears.



Figure 10-20 Edit User Wizard Step 1 of 8 - Select the user that will see the message. Then click Next.

Select the custom message from the drop down menu and click **Next**. Complete all screens and the message will be assigned to the customer. This message will only appear once unless it is setup to repeat or go to a next message in the Custom Message setup screens.

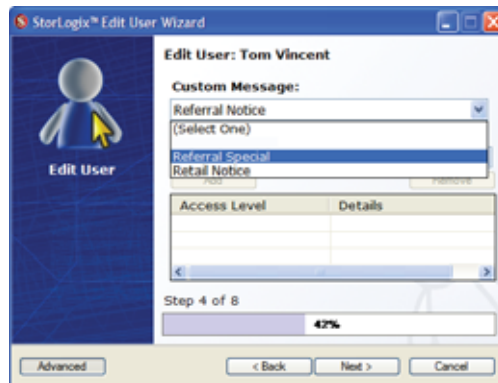


Figure 10-21 Edit User Wizard Step 4 of 8 - Select the custom message that the user will see. Then click Next, going through the remaining screens until done.

Custom Messages Assigned to Devices

Custom messages can also be assigned to specific AI Devices. Click on **16. AI Device Properties** on the Setup Screen.



Figure 10-22 StorLogix Setup Screen - Select 16. AI Device Properties to set a custom message for a keypad.

Click **Next** through the screens until step 7 of 10 in the advanced settings. Select the valid access message to use. Continue pressing **Next** until through all the screens. Then press **Done**. The message will now appear at that device for any users that use it.

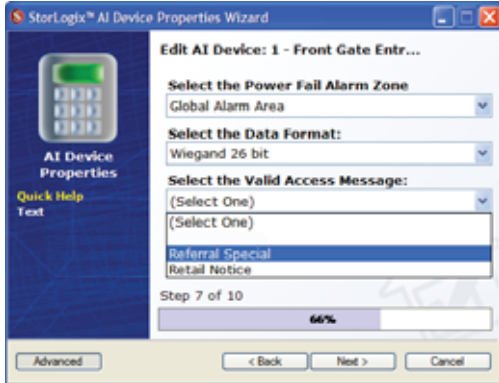


Figure 10-23 AI Device Properties Wizard Step 7 of 10 - Select the custom message that the keypad will use for Valid Access. Then click Next, going through the remaining screens until done.



Alerts

Alerts are messages that can be sent to an email account whenever a specific event occurs in StorLogix.

Email capability must first be setup on the computer. Click on the **Start** button on the desktop and select **Control Panel** from the Start Menu.

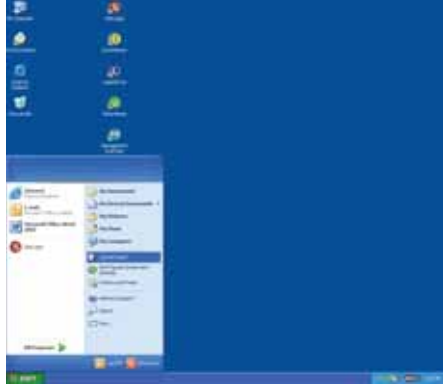


Figure 10-24 Desktop - Select the Control Panel in the Start Menu to setup email capabilities for StorLogix.



REMEMBER

The site must have a high speed internet connection that is always on in order to use some functions in StorLogix. The Alerts function is one of these. Alerts will not work with dial-up internet.

Select **Add/Remove Programs** from the Control Panel.



Figure 10-25 Control Panel - Select Add/Remove Programs.

On the left side of the Add/Remove Program window, select **Add/Remove Windows Components**.



Figure 10-26 Add/Remove Programs - Select Add/Remove Windows Components.

In the Windows Components Wizard, click next to Internet Information Services (IIS) to place a checkmark next to it. Then click the **Details** button.

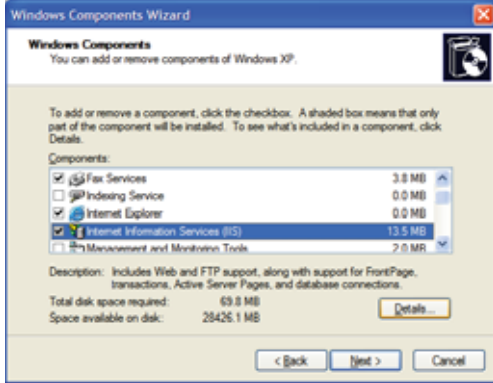


Figure 10-27 Windows Component Wizard - Select Internet Information Services (IIS) and click on the Details button.

In the Internet Information Services (IIS) window, verify that **SMTP Service** is checked. If not, click in the box next to it to select it. Then click **OK**.

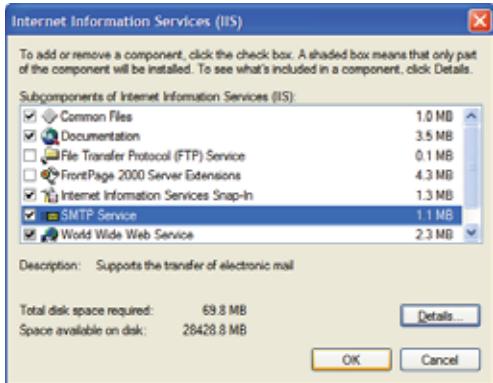


Figure 10-28 Internet Information Services (IIS) - Select the SMTP Service and click OK.

Windows will now add this component to the system. Once it has loaded, click **Finish**. Restart the computer and open StorLogix.

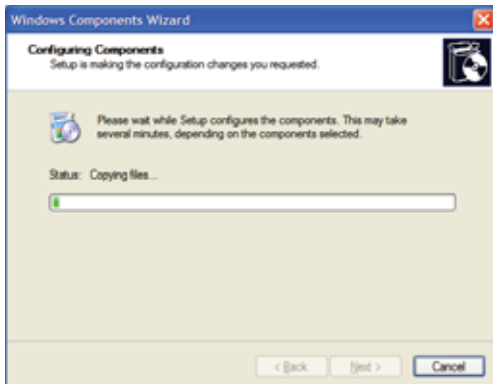


Figure 10-29 Windows Component Wizard - After the installation is complete, click on Finish. Close StorLogix, restart the computer, and then reopen StorLogix.

???????? HINT

Note, the Windows Installation CD may be required when setting up the Internet Information Services SMTP service.

Select **View** on the Menu bar. Then select **Setup Alerts** from the drop down menu.

This wizard only sets up the email addresses that alerts are sent to. The alerts to send are actually setup elsewhere. See the next page for more information on this.



Figure 10-30 StorLogix Main Screen - Select View on the Menu Bar. Then select Setup Alerts.

APPLICATION

Alerts can be setup for specific events so that they alert responsible parties when the event has occurred.

Most commonly, this will be used for alarms. When an alarm goes off, the system can email to a manager's cell phone, email pager, or computer to inform them of the alarm.

A technician troubleshooting the system could have communication alerts emailed to him.

A dealer installing or testing doors on a new site could have all door activity emailed to him, allowing one person with an email pager to test doors on a site.

Sites using wireless door alarms could have the system email the manager when the batteries begin to get low after several years.

Alerts can even be used to watch for specific users. This could be setup if a user is doing suspicious activity, the system would email each time the user came on-site to warn the manager to watch them. This could be especially useful in police investigations where they are trying to apprehend a suspect who is a

Enter a valid email address in the **Insert an Email Address** field and then click on **Add**. Multiple email addresses can be added, but each one will receive an email for every alert sent. Email addresses can be deleted from the list by selecting the address in the list and clicking **Remove**. Click **Done** when finished.



Figure 10-31 Setup Alerts Wizard - Enter an email address and then click Add. Click done when finished.

A dialog box will appear. Click Yes to exit the wizard or No to continue working with alert email addresses.

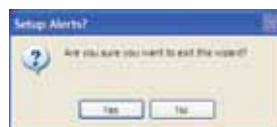


Figure 10-32 Setup Alerts Wizard confirmation dialog box.

Setting up the alert types that will be sent by email are done in two other places.

To send alerts about the activity of a specific user, select **Edit User** from the main StorLogix screen and click through the Edit User wizard to advanced Step 7 of 8. Place a checkmark in the **Alert Notification** box and all events by this user will be emailed as alerts.

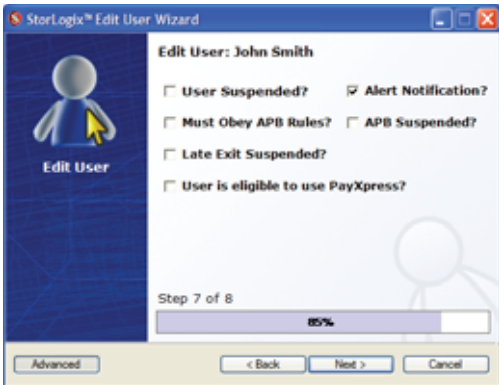


Figure 10-33 Edit User Wizard Step 7 of 8 - Check the Alert Notification box to receive alerts about this user’s activity.

To send alerts about specific event types, select **20. Events to View** from the StorLogix Setup screen (as discussed in Chapter 9). Select an event or events in the Step 1 of 2 and then click **Next**. In Step 2 of 2, select **Yes** in the **Send Email Alerts for this Event** field. This will send an email alert every time this event occurs.

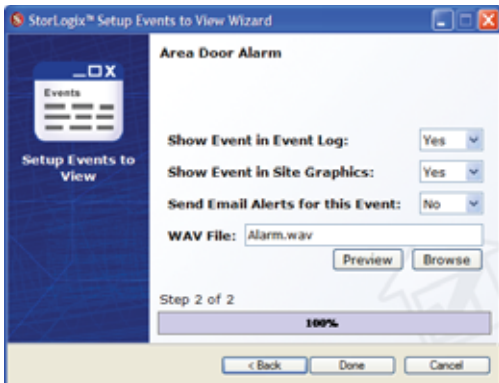
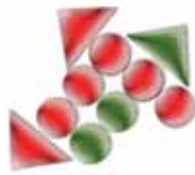


Figure 10-34 Setup Events to View Wizard Step 2 of 2 - Select Yes to view a specific event or events selected in Step 1 of 2.

????????? HINT

The Alerts Function can be a very useful tool for a site if used sparingly. If too many events or users are selected to send alerts, then it can become very overwhelming to the person receiving the emails. It can become impossible to review each email event to determine its importance if the site has set up alerts for a lot of events and users.

It is much better to use this function only for those urgent issues and specific users that need to be dealt with directly.



Inputs to Relays

Inputs to relays allow system inputs such as alarm switches, push buttons, and motion sensors to trigger relays. See the application note in the sidebar for ideas.

Select **Setup** from the Menu Bar. Select **Setup Inputs to Relays** from the drop down list.



APPLICATION

Inputs to Relays can be very useful. Here are some possible uses for them:

A pushbutton inside the office that will trigger the gate to open the gate.

A pushbutton inside the office to trigger a silent alarm.

A wireless pendant that the guard wears while walking the site - push the button and it triggers the panic alarm.

A wireless pendant worn by the manager with a button to open the gate and another to silence alarms. A third button could be a panic alarm.

A pushbutton on the back side of the door to open it.

A motion sensor to open automatic doors.

A switch or motion sensor to turn on lights in a hallway.

Many of these functions can be done without Storlogix, but by using this function, it creates an event in the system that can be tracked and even connected with video of the event.



Figure 10-35 StorLogix Main Screen - Select Setup on the Menu Bar and then Setup Inputs to Relays from the drop down menu.

Select the **Input Point** from the drop down list. This could be a multiplexer channel or an input point on the Falcon XT board.

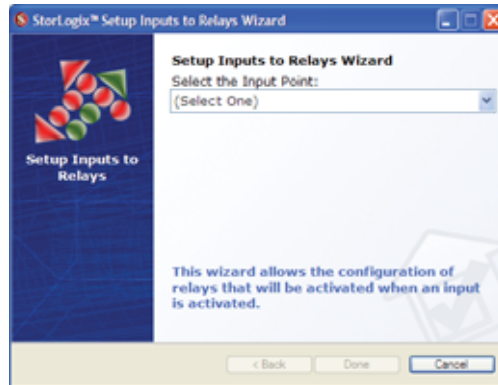


Figure 10-36 Setup Inputs to Relays Wizard - Select the Input Point to trigger the relay.

Select a **Relay to Activate** when the input is closed. Click **Add**.

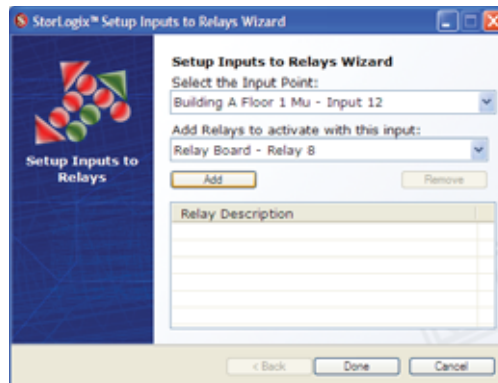


Figure 10-37 Setup Inputs to Relays Wizard - Select the Relay(s) to activate with the input and click Add. Multiple relays can be triggered from the same input.

When all relays for the input have been added, click **Done** to complete the process.

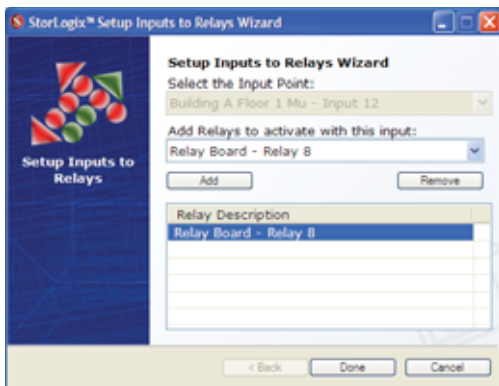


Figure 10-38 Setup Inputs to Relays Wizard - When all relays have been added to the input, click Done.

A dialog box will appear. Click on the **Yes** button to save the Inputs to Relays.

Another dialog box will then appear to confirm that the Inputs to Relays were successfully saved. Click **Yes** to continue adding and editing, click **No** to return to the Setup Screen.



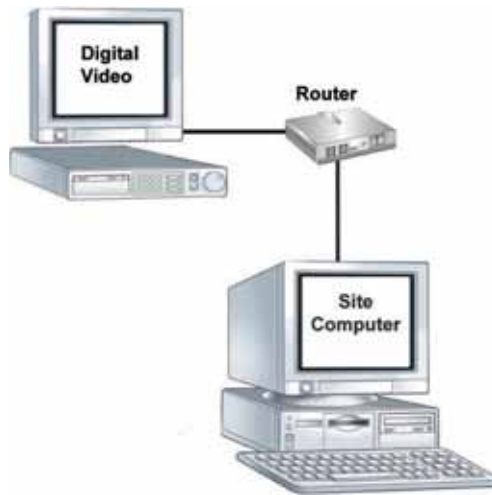
Figure 10-39 Setup Inputs to Relays confirmation dialog boxes.

Networking StorLogix

StorLogix can be setup on a network to allow multiple computers to run StorLogix and/or VideoViewer. Networking multiple software programs can be difficult, so it is very important that a trained IT professional setup any network. PTI Technical Support will not set up the network for you; they will only assist a knowledgeable network IT professional if needed. The following pages include examples that can be used by an IT professional as guidelines for setting up StorLogix on a network.

Example # 1: Networking StorLogix to a DVR

This is a standard setup for a site that has StorLogix integrated with Digital Video.



DVR

- Must be compatible with StorLogix
- Setup IP address in DVR programming. Refer to DVR Manufacturer's instructions for this.
- Setup User Name (if applicable) and password for DVR in DVR programming. Refer to DVR Manufacturer's instructions for this.

Site Computer

- Must have StorLogix and VideoViewer installed and licensed.
- Go in StorLogix Setup Screen and click on DVR. Add a DVR and input a description for the DVR, the DVR Type, IP Address, User Name (if applicable), and Password. See DVR Setup in Chapter 9 of this manual.

CAUTION

Setting up a network and working with programs in a network setting can be very difficult. For this reason, only certified, trained network professionals should attempt to setup StorLogix on a network.

APPLICATION

StorLogix networking can be used for many applications:

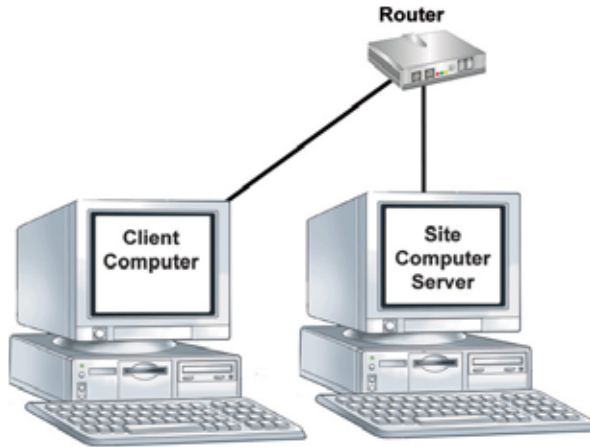
Multiple points-of-sale could be setup at busy sites, allowing multiple operators to use StorLogix at the same time.

An owner with multiple sites could maintain a computer that can remotely access the StorLogix at each site, allowing him to keep track of activity at the sites.

A remote computer with StorLogix and VideoViewer could be placed at a central alarm monitoring or security office to allow remote monitoring and dispatch in case of emergency.

A remote computer with StorLogix could be placed in an on-site manager's apartment allowing instant review of security issues after-hours without having to return to the office.

Example # 2: Networking StorLogix between two computers



Site Computer Server

- Must have StorLogix and VideoViewer installed and licensed.
- Close all programs, including StorLogix, LogixServer, Management Interface, Link program, and VideoViewer.
- In the Start Menu, select Run and type in svrnetcn then click OK.
- This opens the SQL Server Network Utility. Click on the General tab and enable 'Named Pipes' and 'TCP/IP'. Then click OK.
- In the Taskbar, double click on the SQL Server Service Manager. In the 'Server' drop down menu at the top, make sure that the server name matches the name of the local computer.
- Click the 'Stop' button and wait for the status to change to 'Stopped'.
- After it has stopped, click the 'Start/Continue' button to restart the SQL server.
- In the Start Menu, select 'Control Panel' and then 'Windows Firewall'. If this option is not visible, go into the 'Security Center' and click on 'Windows Firewall' under the 'Manager' security settings.
- In the Windows Firewall, click on the 'Exceptions tab.
- Click on 'Add Port' Name the port SQL 1433 and select TCP. Then click OK.
- Click on 'Add Port' again. Name the second port SQL 1434 and select UDP. Then click OK.
- Open StorLogix and select the 'Local' server option under File, Change Database connection on the menu bar.
- This is the computer that the Falcon XT will be connected to.

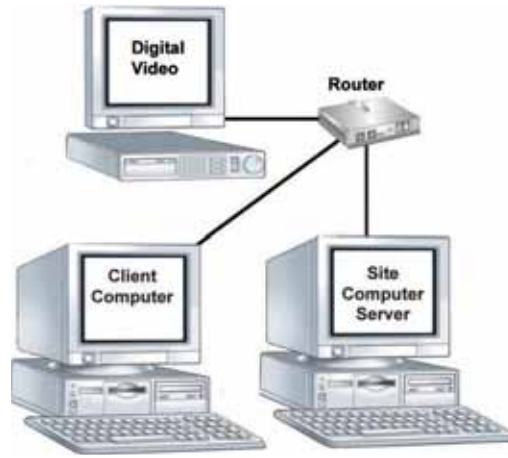
Site Client Computer

- Must have StorLogix and VideoViewer installed and licensed.
- Open StorLogix
- On the Menu Bar, select File and then Change Database Connection.
- Input the Site Computer Server name (or IP address) and test the connection.
- Click Done.

**APPLICATION**

Example # 2 is a standard setup for a site that has StorLogix on multiple computers. This can be used for a second point-of-sale in the office or for a second computer in a manager's apartment.

Example # 3: Networking StorLogix on two computers and a DVR



APPLICATION

Example # 3 is a standard setup for a site that has StorLogix on multiple points-of-sale integrated with Digital Video. It could also be used to have a second computer in a manager's apartment or in a security guard booth allowing security and video monitoring during or after hours.

DVR

- Must be compatible with StorLogix
- Setup IP address in DVR programming. Refer to DVR Manufacturer's instructions for this.
- Setup User Name (if applicable) and password for DVR in DVR programming. Refer to DVR Manufacturer's instructions for this.

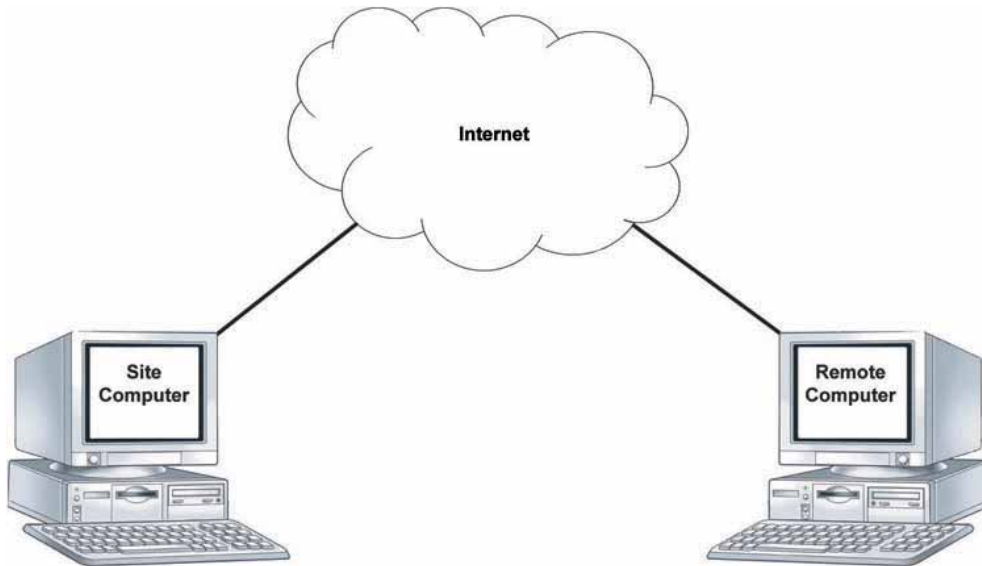
Site Computer Server

- Must have StorLogix and VideoViewer installed and licensed.
- Go in StorLogix Setup Screen and click on DVR. Add a DVR and input a description for the DVR, the DVR Type, IP Address, User Name (if applicable), and Password.
- Close all programs, including StorLogix, LogixServer, Management Interface, Link program, and VideoViewer.
- In the Start Menu, select Run and type in svrnetcn then click OK.
- This opens the SQL Server Network Utility. Click on the General tab and enable 'Named Pipes' and 'TCP/IP'. Then click OK.
- In the Taskbar, double click on the SQL Server Service Manager. In the 'Server' drop down menu at the top, make sure that the server name matches the name of the local computer.
- Click the 'Stop' button and wait for the status to change to 'Stopped'.
- After it has stopped, click the 'Start/Continue' button to restart the SQL server.
- In the Start Menu, select 'Control Panel' and then 'Windows Firewall'. If this option is not visible, go into the 'Security Center' and click on 'Windows Firewall' under the 'Manager' security settings.
- In the Windows Firewall, click on the 'Exceptions tab.
- Click on 'Add Port' Name the port SQL 1433 and select TCP. Then click OK.
- Click on 'Add Port' again. Name the second port SQL 1434 and select UDP. Click OK.
- Open StorLogix and select the 'Local' server option under File, Change Database connection on the menu bar.
- Connect the Falcon XT to this computer.

Site Client Computer

- Must have StorLogix and VideoViewer installed and licensed.
- Open StorLogix
- On the Menu Bar, select File and then Change Database Connection.
- Input the Site Computer Server name (or IP address) and test the connection. Click Done.

Example # 4: Networking StorLogix on two computers via the Internet



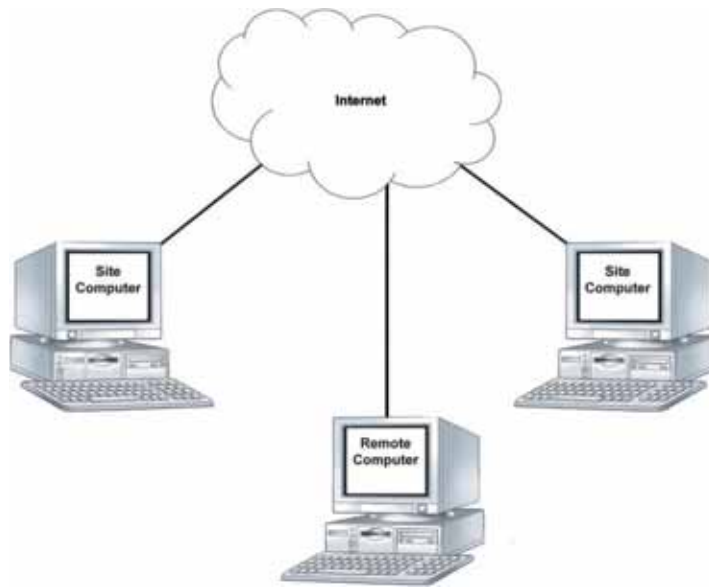
Site Computer

- Must have an 'always on' high-speed internet connection with static IP.
- Must have StorLogix installed and licensed.
- Close all programs, including StorLogix, LogixServer, Management Interface, Link program, and VideoViewer.
- In the Start Menu, select Run and type in svrnetcn then click OK.
- This opens the SQL Server Network Utility. Click on the General tab and enable 'Named Pipes' and 'TCP/IP'. Then click OK.
- In the Taskbar, double click on the SQL Server Service Manager. In the 'Server' drop down menu at the top, make sure that the server name matches the name of the local computer.
- Click the 'Stop' button and wait for the status to change to 'Stopped'.
- After it has stopped, click the 'Start/Continue' button to restart the SQL server.
- In the Start Menu, select 'Control Panel' and then 'Windows Firewall'. If this option is not visible, go into the 'Security Center' and click on 'Windows Firewall' under the 'Manager' security settings.
- In the Windows Firewall, click on the 'Exceptions tab.
- Click on 'Add Port' Name the port SQL 1433 and select TCP. Then click OK.
- Click on 'Add Port' again. Name the second port SQL 1434 and select UDP. Then click OK.
- Open StorLogix and select the 'Local' server option under File, Change Database connection on the menu bar.
- Connect the Falcon XT to this computer

Remote Computer

- Must have an 'always on' high-speed internet connection.
- Must have StorLogix installed and licensed.
- Open StorLogix
- On the Menu Bar, select File and then Change Database Connection.
- Input the Site Computer Server name (or IP address) and test the connection.
- Click Done.

Example # 5: Networking StorLogix between a remote computer and multiple sites via the Internet.



Site Computer at Each Site

- Must have an 'always on' high-speed internet connection with static IP.
- Must have StorLogix installed and licensed.
- for the DVR, the DVR Type, IP Address, User Name (if applicable), and Password.
- Close all programs, including StorLogix, LogixServer, Management Interface, Link program, and VideoViewer.
- In the Start Menu, select Run and type in svrnetcn then click OK.
- This opens the SQL Server Network Utility. Click on the General tab and enable 'Named Pipes' and 'TCP/IP'. Then click OK.
- In the Taskbar, double click on the SQL Server Service Manager. In the 'Server' drop down menu at the top, make sure that the server name matches the name of the local computer.
- Click the 'Stop' button and wait for the status to change to 'Stopped'.
- After it has stopped, click the 'Start/Continue' button to restart the SQL server.
- In the Start Menu, select 'Control Panel' and then 'Windows Firewall'. If this option is not visible, go into the 'Security Center' and click on 'Windows Firewall' under the 'Manager' security settings.
- In the Windows Firewall, click on the 'Exceptions tab.
- Click on 'Add Port' Name the port SQL 1433 and select TCP. Then click OK.
- Click on 'Add Port' again. Name the second port SQL 1434 and select UDP. Then click OK.
- Open StorLogix and select the 'Local' server option under File, Change Database connection on the menu bar.
- Connect the Falcon XT to this computer. Each site must have its own Falcon XT and a different Site Code.

Remote Computer

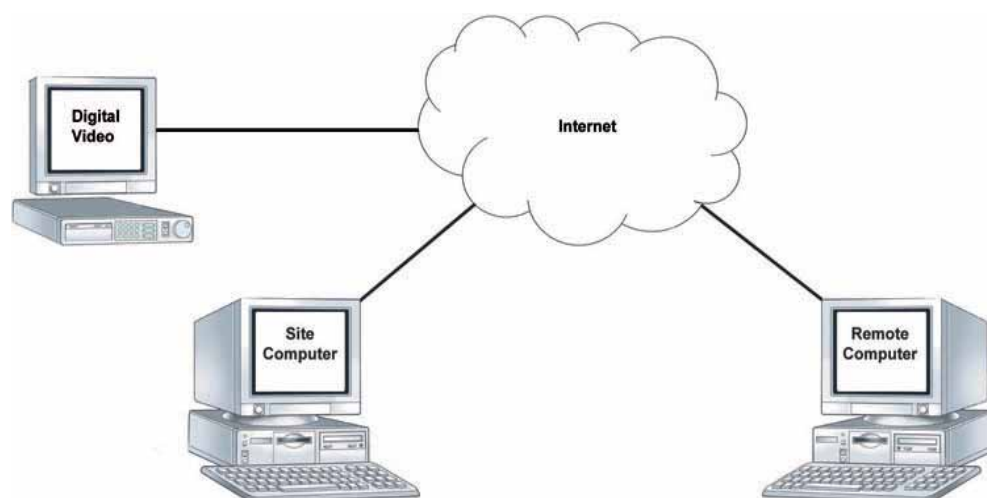
- Must have an 'always on' high-speed internet connection.
- Must have StorLogix installed and licensed.
- Open StorLogix
- On the Menu Bar, select File and then Change Database Connection.
- Input the Site Computer Server name (or IP address) and test the connection. Click Done.
- Repeat the previous step for each site.



APPLICATION

Example # 5 is a setup that might be used by an owner with multiple sites to monitor them from a home office.

Example # 6: Networking StorLogix on two computers and a DVR via the Internet



DVR

- Must have an 'always on' high-speed internet connection with static IP.
- Must be compatible with StorLogix
- Setup IP address in DVR programming. Refer to DVR Manufacturer's instructions for this.
- Setup User Name (if applicable) and password for DVR in DVR programming. Refer to DVR Manufacturer's instructions for this.

Site Computer

- Must have an 'always on' high-speed internet connection with static IP.
- Must have StorLogix and VideoViewer installed and licensed.
- Go in StorLogix Setup Screen and click on DVR. Add a DVR and input a description for the DVR, the DVR Type, IP Address, User Name (if applicable), and Password.
- Close all programs, including StorLogix, LogixServer, Management Interface, Link program, and VideoViewer.
- In the Start Menu, select Run and type in svrnetcn then click OK.
- This opens the SQL Server Network Utility. Click on the General tab and enable 'Named Pipes' and 'TCP/IP'. Then click OK.
- In the Taskbar, double click on the SQL Server Service Manager. In the 'Server' drop down menu at the top, make sure that the server name matches the local computer.
- Click the 'Stop' button and wait for the status to change to 'Stopped'.
- After it has stopped, click the 'Start/Continue' button to restart the SQL server.
- In the Start Menu, select 'Control Panel' and then 'Windows Firewall'. If this option is not visible, go into the 'Security Center' and click on 'Windows Firewall' under the 'Manager' security settings.
- In the Windows Firewall, click on the 'Exceptions tab.
- Click on 'Add Port' Name the port SQL 1433 and select TCP. Then click OK.
- Click on 'Add Port' again. Name the second port SQL 1434 and select UDP. Click OK.
- Open StorLogix and select the 'Local' server option under File, Change Database connection on the menu bar.
- Connect the Falcon XT to this computer.

Remote Computer

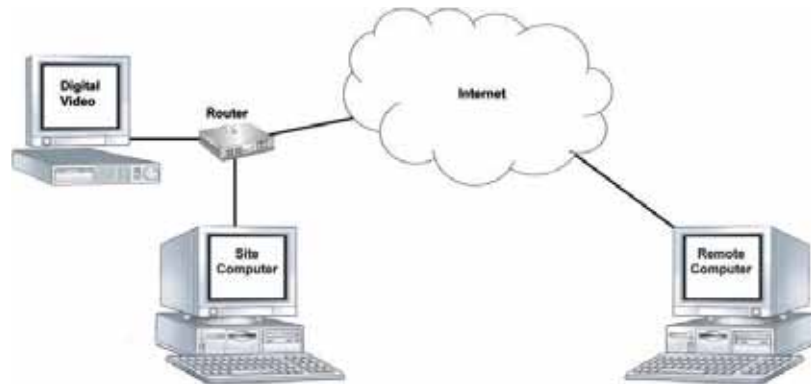
- Must have an 'always on' high-speed internet connection.
- Must have StorLogix and VideoViewer installed and licensed.
- Open StorLogix
- On the Menu Bar, select File and then Change Database Connection.
- Input the Site Computer Server name (or IP address) and test the connection. Click Done.



APPLICATION

Example # 6 is a setup that might be used by an owner with a single site to monitor the site from his home office. It could also be used to provide remote monitoring by an alarm company or in a security guard booth.

Example # 7: Networking StorLogix on two computers and a DVR via the Internet and a Router



Router

- Must have an 'always on' high-speed internet connection with static IP.
- Must set up Port Forwarding

DVR

- Must be compatible with StorLogix
- Setup IP address in DVR programming. Refer to DVR Manufacturer's instructions for this.
- Setup User Name (if applicable) and password for DVR in DVR programming. Refer to DVR Manufacturer's instructions for this.

Site Computer

- Must have StorLogix and VideoViewer installed and licensed.
- Go in StorLogix Setup Screen and click on DVR. Add a DVR and input a description for the DVR, the DVR Type, IP Address, User Name (if applicable), and Password.
- Close all programs, including StorLogix, LogixServer, Management Interface, Link program, and VideoViewer.
- In the Start Menu, select Run and type in svrnetcn then click OK.
- This opens the SQL Server Network Utility. Click on the General tab and enable 'Named Pipes' and 'TCP/IP'. Then click OK.
- In the Taskbar, double click on the SQL Server Service Manager. In the 'Server' drop down menu at the top, make sure that the server name matches the local computer.
- Click the 'Stop' button and wait for the status to change to 'Stopped'.
- After it has stopped, click the 'Start/Continue' button to restart the SQL server.
- In the Start Menu, select 'Control Panel' and then 'Windows Firewall'. If this option is not visible, go into the 'Security Center' and click on 'Windows Firewall' under the 'Manager' security settings.
- In the Windows Firewall, click on the 'Exceptions tab.
- Click on 'Add Port' Name the port SQL 1433 and select TCP. Then click OK.
- Click on 'Add Port' again. Name the second port SQL 1434 and select UDP. Click OK.
- Open StorLogix and select the 'Local' server option under File, Change Database connection on the menu bar.
- Connect the Falcon XT to this computer.

Remote Computer

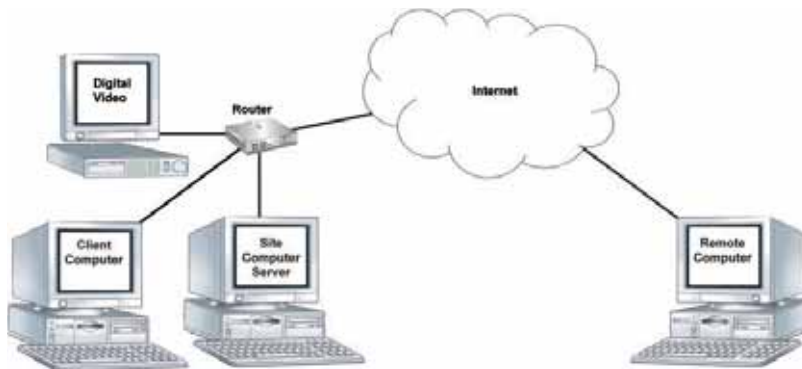
- Must have an 'always on' high-speed internet connection.
- Must have StorLogix and VideoViewer installed and licensed.
- Open StorLogix
- On the Menu Bar, select File and then Change Database Connection.
- Input the Site Computer Server name (or IP address) and test the connection. Click Done.



APPLICATION

Example # 7 is a setup that might be used by an owner with a single site to monitor the site from his home office. It could also be used to provide remote monitoring by an alarm company or in a security guard booth.

Example # 8: Networking StorLogix on multiple computers and a DVR via the Internet and a Router



Router

- Must have an 'always on' high-speed internet connection with static IP.
- Must set up Port Forwarding

DVR

- Must be compatible with StorLogix
- Setup IP address in DVR programming. Refer to DVR Manufacturer's instructions for this.
- Setup User Name (if applicable) and password for DVR in DVR programming. Refer to DVR Manufacturer's instructions for this.

Site Computer Server

- Must have StorLogix and VideoViewer installed and licensed.
- Go in StorLogix Setup Screen and click on DVR. Add a DVR and input a description for the DVR, the DVR Type, IP Address, User Name (if applicable), and Password.
- Close all programs, including StorLogix, LogixServer, Management Interface, Link program, and VideoViewer.
- In the Start Menu, select Run and type in svrnetcn then click OK.
- This opens the SQL Server Network Utility. Click on the General tab and enable 'Named Pipes' and 'TCP/IP'. Then click OK.
- In the Taskbar, double click on the SQL Server Service Manager. In the 'Server' drop down menu at the top, make sure that the server name matches the local computer.
- Click the 'Stop' button and wait for the status to change to 'Stopped'.
- After it has stopped, click the 'Start/Continue' button to restart the SQL server.
- In the Start Menu, select 'Control Panel' and then 'Windows Firewall'. If this option is not visible, go into the 'Security Center' and click on 'Windows Firewall' under the 'Manager' security settings.
- In the Windows Firewall, click on the 'Exceptions tab'.
- Click on 'Add Port' Name the port SQL 1433 and select TCP. Then click OK.
- Click on 'Add Port' again. Name the second port SQL 1434 and select UDP. Click OK.
- Open StorLogix and select the 'Local' server option under File, Change Database connection on the menu bar.

Client Computer

- Must have StorLogix and VideoViewer installed and licensed.
- Open StorLogix. On the Menu Bar, select File and then Change Database Connection.
- Input the Site Computer Server name (or IP address) and test the connection.

Remote Computer

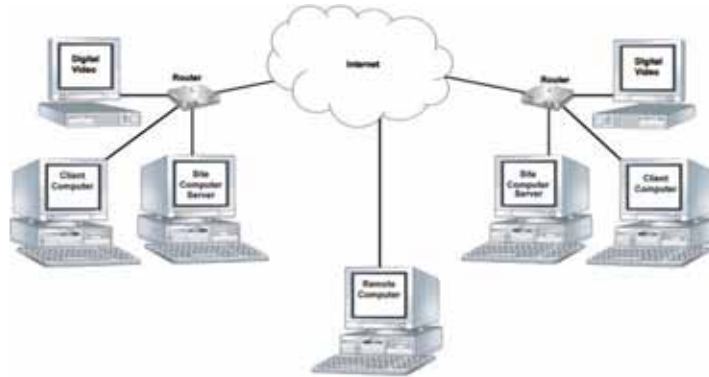
- Must have an 'always on' high-speed internet connection.
- Must have StorLogix and VideoViewer installed and licensed.
- Open StorLogix. On the Menu Bar, select File and then Change Database Connection.
- Input the Site Computer Server name (or IP address) and test the connection. Click Done.



APPLICATION

Example # 8 is a setup that might be used by site with multiple points-of-sale and an owner with a single site to monitor the site from his home office. It could also be used to provide remote monitoring by an alarm company or in a security guard booth or to have a computer in a manager's apartment for after-hours monitoring.

Example # 9: Networking StorLogix between Many Sites



Router at Each Site

- Must have an 'always on' high-speed internet connection with static IP.
- Must set up Port Forwarding

DVR at Each Site

- Must be compatible with StorLogix
- Setup IP address in DVR programming. Refer to DVR Manufacturer's instructions for this.
- Setup User Name (if applicable) and password for DVR in DVR programming. Refer to DVR Manufacturer's instructions for this.

Site Computer Server at Each Site

- Must have StorLogix and VideoViewer installed and licensed.
- Go in StorLogix Setup Screen and click on DVR. Add a DVR and input a description for the DVR, the DVR Type, IP Address, User Name (if applicable), and Password.
- Close all programs, including StorLogix, LogixServer, Management Interface, Link program, and VideoViewer.
- In the Start Menu, select Run and type in svrnetcn then click OK.
- This opens the SQL Server Network Utility. Click on the General tab and enable 'Named Pipes' and 'TCP/IP'. Then click OK.
- In the Taskbar, double click on the SQL Server Service Manager. In the 'Server' drop down menu at the top, make sure that the server name matches the local computer.
- Click the 'Stop' button and wait for the status to change to 'Stopped'.
- After it has stopped, click the 'Start/Continue' button to restart the SQL server.
- In the Start Menu, select 'Control Panel' and then 'Windows Firewall'. If this option is not visible, go into the 'Security Center' and click on 'Windows Firewall' under the 'Manager' security settings.
- In the Windows Firewall, click on the 'Exceptions tab.
- Click on 'Add Port' Name the port SQL 1433 and select TCP. Then click OK.
- Click on 'Add Port' again. Name the second port SQL 1434 and select UDP. Click OK.
- Open StorLogix and select the 'Local' server option under File, Change Database connection on the menu bar.
- A Falcon XT will be connected to this computer at each site.

Client Computer at Each Site

- Must have StorLogix and VideoViewer installed and licensed.
- Open StorLogix. On the Menu Bar, select File and then Change Database Connection.
- Input the Site Computer Server name (or IP address) and test the connection.

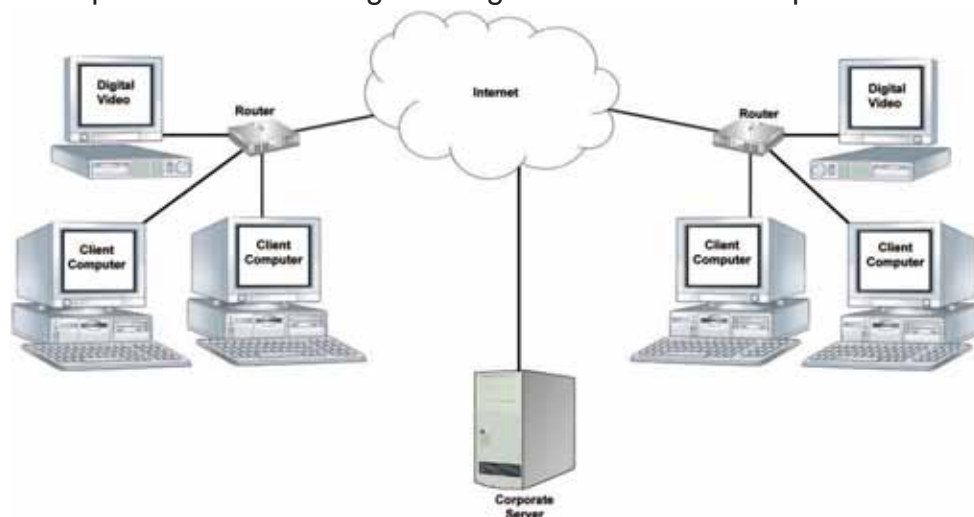
Remote Computer

- Must have an 'always on' high-speed internet connection.
- Must have StorLogix and VideoViewer installed and licensed.
- Open StorLogix. On the Menu Bar, select File and then Change Database Connection.
- Input the Site Computer Server name (or IP address) and test the connection. Click Done.

APPLICATION

Example # 9 is similar to Example # 8, only it is for a company with multiple sites that wants remote monitoring by a central monitoring station or has an owner that wants to monitor activity at multiple sites.

Example # 9: Networking StorLogix with a Central Corporate Server



Router at Each Site

- Must have an 'always on' high-speed internet connection with static IP.
- Must set up Port Forwarding

DVR at Each Site

- Must be compatible with StorLogix
- Setup IP address in DVR programming. Refer to DVR Manufacturer's instructions for this.
- Setup User Name (if applicable) and password for DVR in DVR programming. Refer to DVR Manufacturer's instructions for this.

Corporate Server

- Must have StorLogix and VideoViewer installed and licensed.
- Go in StorLogix Setup Screen and click on DVR. Add a DVR and input a description for the DVR, the DVR Type, IP Address, User Name (if applicable), and Password.
- Close all programs, including StorLogix, LogixServer, Management Interface, Link program, and VideoViewer.
- In the Start Menu, select Run and type in svrnetcn then click OK.
- This opens the SQL Server Network Utility. Click on the General tab and enable 'Named Pipes' and 'TCP/IP'. Then click OK.
- In the Taskbar, double click on the SQL Server Service Manager. In the 'Server' drop down menu at the top, make sure that the server name matches the local computer.
- Click the 'Stop' button and wait for the status to change to 'Stopped'.
- After it has stopped, click the 'Start/Continue' button to restart the SQL server.
- In the Start Menu, select 'Control Panel' and then 'Windows Firewall'. If this option is not visible, go into the 'Security Center' and click on 'Windows Firewall' under the 'Manager' security settings.
- In the Windows Firewall, click on the 'Exceptions tab'.
- Click on 'Add Port' Name the port SQL 1433 and select TCP. Then click OK.
- Click on 'Add Port' again. Name the second port SQL 1434 and select UDP. Click OK.
- Open StorLogix and select the 'Local' server option under File, Change Database connection on the menu bar.

Client Computer(s) at Each Site

- Must have an 'always on' high-speed internet connection with static IP.
- Must have StorLogix and VideoViewer installed and licensed.
- Open StorLogix. On the Menu Bar, select File and then Change Database Connection.
- Input the Corporate Server name (or IP address) and test the connection.
- The Falcon XT for each site is connected to one main client computer at each site. Each Site must have its own Falcon XT and each Falcon XT must have a unique Site Code.



APPLICATION

Example # 10 is a specialty setup that could be used by larger companies that have many sites all connected to a central corporate server.

Interface to TaskMaster

StorLogix can easily be interfaced to TaskMaster Management Software. This interface allows units to be automatically locked out when the client does not pay their bills. It also automatically adds clients to the StorLogix as they are entered in TaskMaster.

To perform this interface, complete the following steps:

1. Be sure that TaskMaster is installed and that it is at least version 1.542 or higher.
2. Check the 'C:' drive on the computer. Verify that there is a F2000 folder. If this folder does not exist, create one.

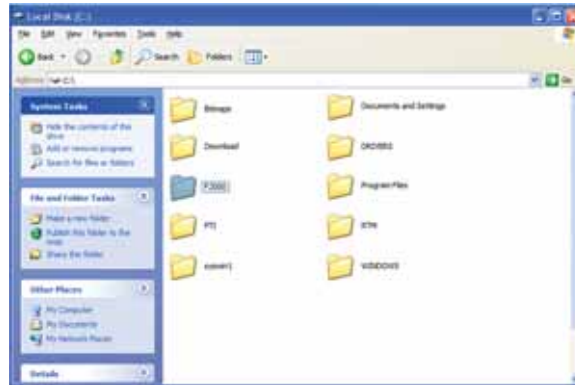


Figure 10-40 Verify that there is a F2000 folder in the root of the C: drive.

3. In the TaskMaster program, select 'Utilities' from the menu bar and select System Setup > Registration from the drop down menu. Verify that Gate Interface is listed as StorLogix. If there is anything else in that field, call PTI Technical Support to change this.

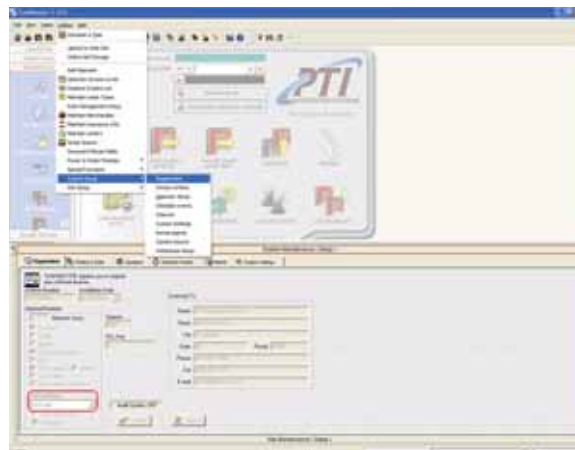


Figure 10-41 Verify that the StorLogix interface is activated in the Registration screen of Site Setup in TaskMaster.



REMEMBER

Because TaskMaster is manufactured by the same company that makes StorLogix and the Falcon XT, the PTI TaskMaster Interface is true product integration and so it generally works more smoothly than interfaces with other types of software.

If you do not already have TaskMaster Management Software, contact PTI at (800) 331-6224 to get a free demonstration copy.



APPLICATION

When TaskMaster is interfaced to StorLogix, the PayXpress function may be used.* This function allows customers to pay their bills at the gate using a credit card. PayXpress immediately verifies the credit card transaction allowing instant approval or decline. It also bills all fees and charges to the credit card along with the regular billing amount - this means fees don't get waived and more money goes into your pocket.

* PayXpress is a module in TaskMaster that must be purchased separately and has additional requirements. For more information on PayXpress, contact PTI at (800) 331-6224.



APPLICATION

When TaskMaster is interfaced to StorLogix, the StorLogix Event Log can be viewed in TaskMaster eliminating the need to switch between programs.

Interface to other Accounting Software

StorLogix can also be interfaced to many other brands of Accounting Software. The interface works similar to the TaskMaster Interface by allowing units to be automatically locked out when the client does not pay their bills and automatically adding clients to the StorLogix as they are entered in accounting software. The only real difference is that the interface setup may be a little more complicated.

To perform this interface, complete the following steps:

1. Be sure that the Management Software is loaded on the computer and licensed with the interface already activated by them.
2. Open the PTI Easy Link program by double clicking on the icon on the desktop or by selecting it from the programs menu.



Figure 10-42 PTI EasyLink Icon

3. When the EasyLink program opens, select the Accounting Software that will be interfaced to the Falcon XT from the list on the General Tab.



Figure 10-43 PTI EasyLink General Tab.

????????? HINT

If the interface needs to be setup in a network situation, contact PTI Technical Support before trying to setup the interface so that they can help.

CAUTION

Many Accounting Software companies charge for this interface. This must be paid in advance and setup by the Accounting software manufacturer. Contact them before beginning this process to make sure that you have an activated interface. PTI does not charge a fee for the interface, but we also cannot assist with this as it is a function of the accounting software.

4. Select the Settings Tab. In the settings tab, under Link Type, select *Local - With Falcon 2000*. If the site has individual door alarms on the site, select *Using Individual Door Alarms* under the Alarms section.

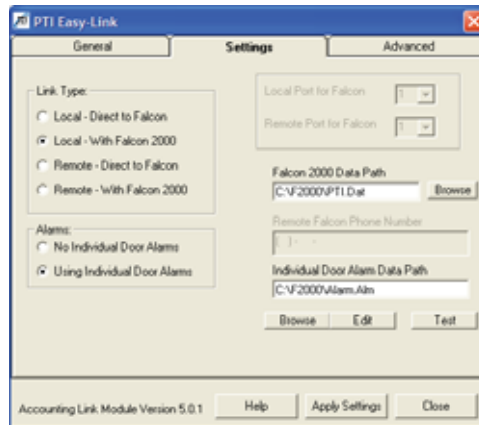


Figure 10-44 PTI EasyLink Settings Tab.

5. Select the Advanced Tab. The *Import Data File Name and Path* and *Result Data File Path* can be updated here if the Interace is setup across a network. Click **Apply Settings** to complete the process.

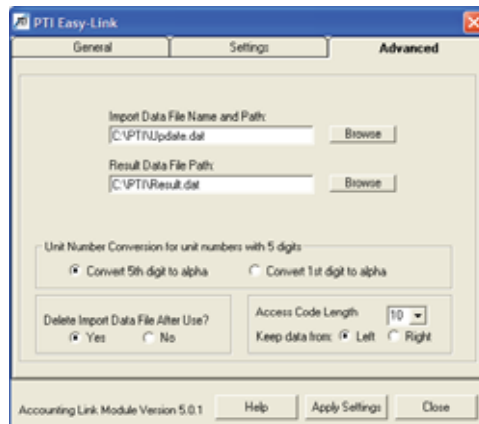


Figure 10-45 PTI EasyLink Advanced Tab.

6. Next, open the Management Interface program by clicking on the Management Interface Icon on the desktop or by opening it in the Programs menu.



Figure 10-46 Management Interface Program Icon

- When the Management Interface window appears, click on Setup.

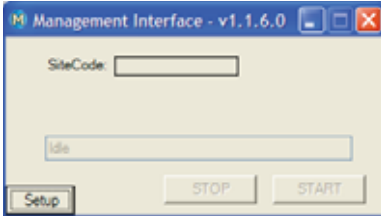


Figure 10-47 Management Interface Program. Click on Setup.

- The site that was setup in StorLogix should appear in the Setup window. Click on the site and then click on **Edit**.



Figure 10-48 Management Interface Setup. Select the Site and click Edit.

- In the Setup2 screen, click on the Active button to activate the Interface. Enter the path information for the Input File. This is the same as the Falcon 2000 data path found on the Settings tab of the EasyLink program (see previous page). Enter the paths for the Activity Log, Error Log, Result File, and Event File. See the Hint in the sidebar for more information on these. Click **Save** when done.

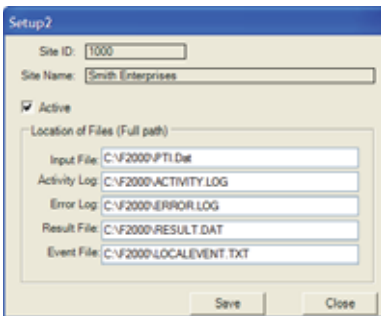


Figure 10-49 Management Interface Setup screen 2. Click on Active and then input the file and log paths. Then click Save.

- Click **Close** to close the Interface Setup. The Management Interface will begin processing.



Figure 10-50 Management Interface Setup screen activated. Click on Close to begin the processing.

???????
HINT

The Activity Log, Error Log, Result File, and Event File are used for tracking and troubleshooting the Management Interface. Because this interface is a one way flow of information from the Accounting Software to the PTI StorLogix program, we have no control over the information coming into the StorLogix program. This can make troubleshooting difficult. To help track what is happening in the information transfer from the Accounting Software, we can keep these logs and files to help troubleshoot if there is a problem. It is a good idea to create these files and keep them on the computer. If these fields are left blank, then this information is not stored and may delay troubleshooting if there is ever a problem with the interface.

LogixScript

LogixScript is one of the most powerful functions of the entire StorLogix system. It allows the administrator to create almost any function that they can think of by writing custom scripts using If/Then commands.

LogixScript lines are reviewed 4 times per second by the system. This means that multiple commands, and sets of commands can occur almost simultaneously.

Each LogixScript function is created by writing a set of commands or lines of script. Each line consists of one or two 'If' statements and one 'Then' statement. An example of this concept might be: "IF the manager leaves the site AND IF the lights are still on, THEN turn the lights off." The actual script must be a little more specific than the example, including relay numbers and access areas, but the concept is the same.

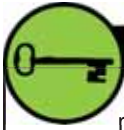
Since there are almost unlimited combinations of LogixScript options, we will demonstrate how to use LogixScript by creating a custom script.

To begin, it is important to outline the desired function. In our example, Tom Vincent, the site manager likes to have hot coffee when he arrives in the morning. He would like the system to automatically activate his coffee maker about 15 minutes before he gets to the site.

After deciding what the function should be, then it becomes important to outline the conditions for the function. In our example, the Mr. Vincent sometimes arrives early and brews his own coffee. On these occasions, he does not want the system to try to start the coffee maker again. Also, sometimes, he has to visit another site in the morning, so he doesn't want the coffee maker to stay on and burn up.

Now that the parameters are decided upon, we can begin the process of creating a script. It is a good idea to create a list of the intended steps and conditions:

- If it is 7:30 am and Mr. Vincent is not yet on-site, start the coffee maker.
- If Mr. Vincent is already on-site at 7:30 am, don't start the coffee maker.
- If it is 8:30 am and Mr. Vincent still is not on-site, turn it off.



???????? HINT

LogixScript doesn't require an expert programmer. All that is required is the ability to think through the steps in a logical order and a little bit of practice.

To create a custom function, it is a good idea to write down the desired outcome and all of the variables before trying to write a script. Consider which relays might be involved, what devices it will affect, which users does it apply to, and what are the possible implications to uninformed variables.

A single LogixScript function may involve several steps, each requiring its own script. With careful pre-planning and a logical input order, just about any custom function desired can be made to happen.

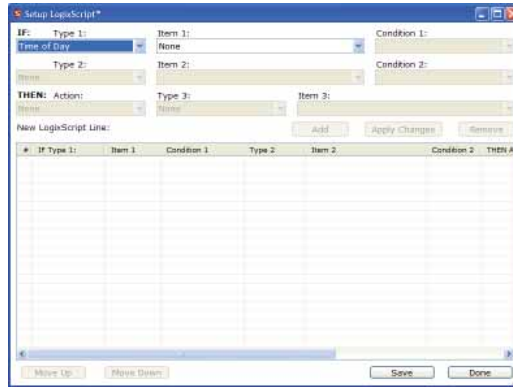
It may take some experimentation to get the outcome that is desired. Steps must be in order, and all factors must be considered.



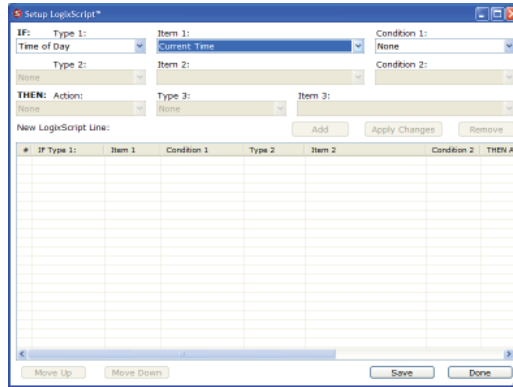
CAUTION

It is possible to put LogixScript into a logic-loop that can cause problems with the system. This could include: failure of the script or other scripts to function, locking or holding relays preventing access and egress, excessive creation of events that lock up the database or slow down the computer, or other similar issues. It is a good idea to back-up the system prior to adding a LogixScript command and it is a good idea to carefully test each set of commands to make sure that they perform as expected.

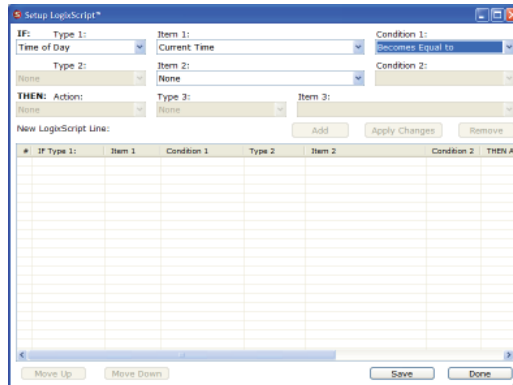
Begin writing the first line of script. The first parameter is “If it is 7:30 am and Mr. Vincent is not on-site, start the coffee maker.” This is actually two conditions: “If it is 7:30 am” and “If Mr. Vincent is not on-site”. We must deal with these separately. In the first ‘If’ field ‘Type 1’, select **Time of Day**.



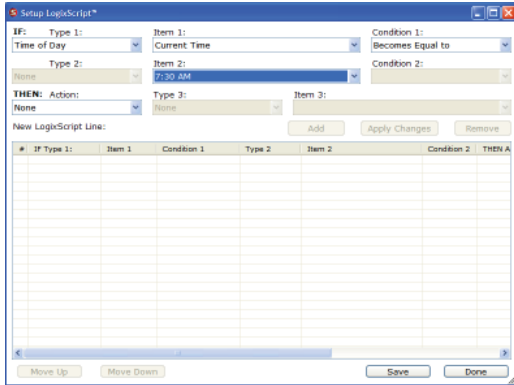
In the next field ‘Item 1’, select **Current Time**.



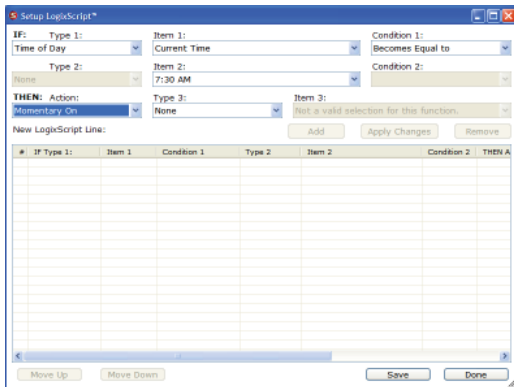
In the ‘Condition 1’ field, select **Becomes Equal To**.



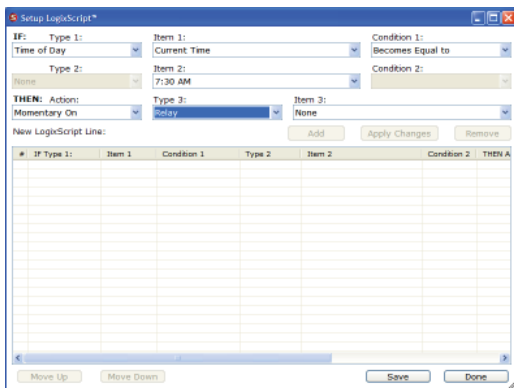
In the 'Item 2' field, select the desired time: **7:30 am**.



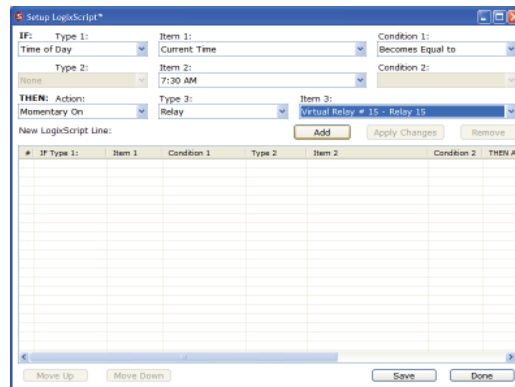
Under the 'Action Field', select **Momentary On**.



Under 'Type 3', select **Relay**.



Finally, in 'Item 3', select a virtual relay. This relay should have already been created earlier in the Relay setup discussed in chapter 4. A virtual relay is just an ON/OFF switch in the programming. In this case, we have to create a two part command "If time is 7:30 am" and "If Mr. Vincent is not on-site". To accomplish this, we create a virtual relay. If the time becomes 7:30 am, trigger this virtual relay to ON. We will then create a command to say, If this relay comes on and Mr. Vincent is not On-site, then start the coffee maker. If Mr. Vincent just wanted the coffee maker to come on every day at 7:30, this virtual relay would not be needed. However, the second condition requires it. To enter this line of script, click **Add**.



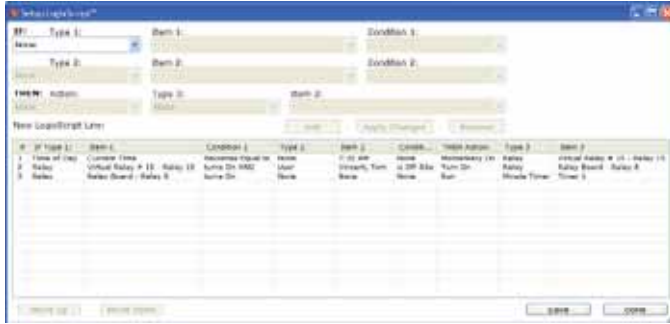
Now the first line of script has been created. If the time becomes 7:30 am, then virtual relay # 15 will switch on momentarily and then off.



Create the next condition. IF Relay, Virtual Relay # 15, Turns On AND User, Tom Vincent is off-site, Then Turn On Relay, # 8. Relay # 8 is the one wired to the Coffee Maker.



At this point, we could stop. This would automatically turn on the coffee maker every day at 7:30 am if Tom Vincent is not on-site. However, there is another desired condition: “If it is 8:30 am and Mr. Vincent still is not on-site, turn off the coffee maker.” To do this, we create a line of script that says “If Relay, Relay # 8, Turns On, Then Run Minute Timer, Timer 1.” This starts a timer that counts up minutes.



Now, set the condition “If Minute Timer, Timer 1, Becomes Equal To Numeric Value 60, Then, Momentary On Relay, Virtual Relay # 16.” This will automatically turn on Virtual Relay # 16 one hour after the coffee maker turns on. This is similar to lines 1 and 2 of the script where it took a virtual relay to accomplish the two commands. In this case, we again have two commands: “If the coffee maker has been on for 60 minutes” AND “Mr. Vincent still hasn’t come on-site”.



Now we create the second part: “If Virtual Relay # 16 Turns On AND User, Tom Vincent is Off-Site, Turn Off Relay # 8. This will turn off relay # 8 (turning off the coffee maker) if Mr. Vincent still isn’t on-site 1 hour after the coffee maker turned on.



The final step of the process is to reset the timer. Timers continue counting to infinity unless reset. Running a timer starts it if a condition is met, and it will continue to run. Resetting a timer restarts it a zero and it will automatically begin counting again unless the condition that started it is not met. In our example, if Relay 8 is on, the timer will count. If Relay 8 is off, the timer will stop counting. Therefore, after we stop the timer in step 5, by turning off the relay, we still need to reset it to zero so that it will be ready again the next day to count up to 60. If we don't reset it, then the coffee maker will never again turn off because the timer will never again reach 60 (because it will be far past that number). To reset the timer, we enter a line that says "If Relay # 8 turns off, Then Reset Minute Timer, Timer 1." This will reset the timer to zero so it is ready to be used again.

HINT

This coffee maker example could be used to turn on air conditioning or heating as well as lights or other office fixtures.

When complete, click the **Save** button and then the **Done** button.

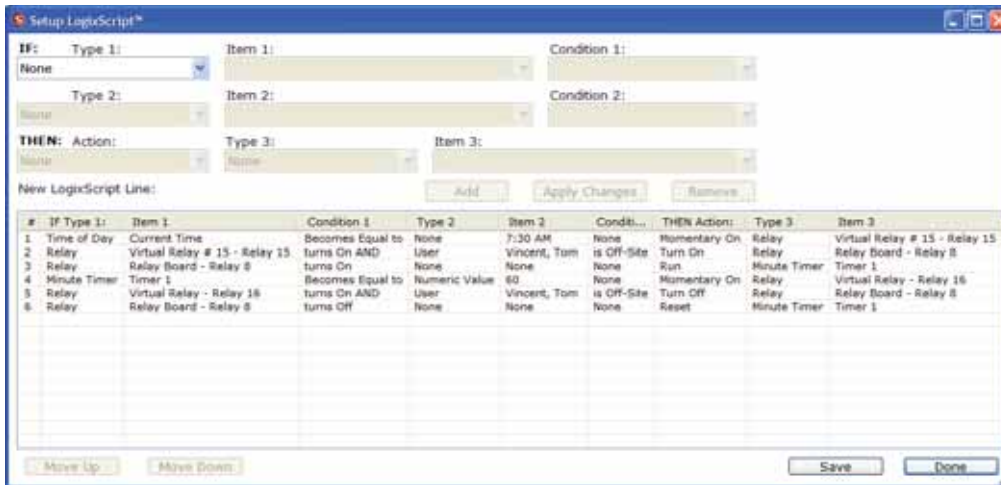


A dialog box will appear. Click on the **Yes** button to save the change(s).

Another dialog box will then appear to confirm that the LogixScript changes were successfully saved. Click **OK**.



This is just one example of the many things that can be setup using LogixScript.



StorLogix runs through LogixScript four times per second. During this, it will review each line of script in order, executing each 'Then' function every time the 'If' conditions are met.

It is very important that each line of script be in order or the command may not function in the expected way (if at all).

Lines of script can be moved up and down in order by clicking on the line to highlight it and clicking on the **Move Up** or **Move Down** buttons.

Mistakes can be corrected by selecting a line of script and making changes. Then click on **Apply Changes**.

It is a good idea to click **Save** after each line of script is entered, so that it is not lost or accidentally changed as the programming continues.



REMEMBER

Remember that it is a good idea to carefully plot out the function that is desired. Remember, that it may affect other parts of the system.

If you trigger the gate open using LogixScript, then it bypasses all other system functions. The gate would then be open, even if it should be closed during that time of day.

If you write out the plan and carefully think through each step, then this can be a very powerful tool for customizing the site.

LogixScript 'If' Functions:

# of Users in Access Area	'Then' function can be based on being or becoming greater than, less than, equal to, unequal to the number of users in that specific area. Must choose the area in question.
Access Area	'Then' function can be based on being or becoming in alarm or not in alarm state. Must select the area in question.
Alarm Zone	'Then' function can be based on being or becoming in alarm or not in alarm state. Must select the area in question.
Card	'Then' function can be based on a specific card (or code) being input at an AI Device.
Counter	There are 50 counters in the system. Each counter can be incremented or decremented by 1 as a 'Then' function. As an 'If' function, it can be based on the counter being or becoming greater than, less than, equal to, or unequal to a specific numeric value, timer, or other number.
Input	'Then' function can be based on a specific input being or becoming active, inactive, or check-in fail. Must select input.
Lighting Area	'Then' function can be based on a specified lighting area being or becoming turned on or off. Must select the lighting area.
Maximum in Area	Allows the 'Then' function to be based on the number of users in a particular area.
Numeric Value	This cannot be used as a first 'If' function but can be used as a second 'If' condition. For example, If counter becomes equal to numeric value 25, then... The numeric value must be set.
Relay	'Then' function can be based on a specific relay being on or off, or turning on or off. Must choose the relay.
System Function	These include system startup and ticks of time.
Time of Day	'Then' function can be based on a specific time (hours and minutes) during the day.
Time Schedule	'Then' function can be based on a time schedule being or becoming active or inactive.
Timers	There are 50 timers in the system. They can be uses as Hour Timers, Minute Timers, Second Timers, or tenths of a second timers. Timers are run or reset as a 'Then' function. As an 'If' function, it is based on the timer being or becoming equal to, greater than, less than, or unequal to a certain amount of time set as a numeric value.
Unit	'Then' function can be based on a specific unit being or becoming occupied, vacant, in alarm state or alarm being cleared.
User	'Then' function can be based on a specific user being or coming on-site, offsite, suspended, or unsuspending.
User In Area	'Then' function can be based on a specific user being in or going into or leaving a specific area.
_____ And	Some 'If' commands allow a second 'If' command by using 'And'. For example, if the user enters the site AND unit enters alarm, then...
_____ Or	Some 'If' commands allow a second 'If' command by using 'Or'. For example, if the user enters the site or if their unit enters alarm, then...

LogixScript 'Then' Functions:

Clear	This 'Then' function is used to clear Users from Access Areas or it can clear Users or Units from the site when the 'If' conditions are met.
Decrement	This 'Then' function reduces a counter by 1 when the 'If' conditions are met. The counter must be specified.
Increment	This 'Then' function increases a counter by 1 when the 'If' conditions are met. The counter must be specified.
Momentary On	This 'Then' function triggers a specified relay on one time and then turns it right back off in the same second when the 'If' conditions are met.
Momentary Off	This 'Then' function triggers a specified relay off one time and then turns it right back off in the same second when the 'If' conditions are met.
Reset	This 'Then' function starts a timer back at zero. The timer then begins running again. Timers are either on (when the 'If' conditions are met) or off (when the 'If' conditions are not met). If a timer is on, then it is always counting up.
Run	This 'Then' function starts a timer where it last left off. Timers are either on (when the 'If' conditions are met) or off (when the 'If' conditions are not met). If a timer is on, then it is always counting up.
Send Alert	This 'Then' function sends an alert to the person(s) setup in the Alert function when the 'If' conditions are met.
Silence	This 'Then' function is used to silence a specific alarm zone when the 'If' conditions are met.
Turn Off	This 'Then' function turns a specified relay off when the 'If' conditions are met.
Turn On	This 'Then' function holds a specified relay on when the 'If' conditions are met. The relay will stay on until another LogixScript command turns it off. Note, if a relay is held on using this function, then it cannot be overridden by any other system function such as entering a code at the keypad, or the Open door/gate function.



APPLICATION

A manager could enter a card in the system and use it to clear all users off-site as the manager checks out at the exit keypad when they leave at night. They could also set a card to silence alarms when they present it at any keypad.

A guard tour could be setup by using a timer to start when a certain card is presented at a keypad. If the timer reaches a certain amount of time such as 30 minutes, then an alarm sounds unless the card has been presented at another keypad.

LogixScript could be used to send a reminder to do gate maintenance. Each time the relay is triggered, it could increment a counter. When the counter reaches a certain point, then LogixScript can send an alert that it is time to call the gate company.

For more information on these suggested applications and more, see the PTI StorLogix Applications booklet.

CHAPTER 11: TROUBLESHOOTING

- **TROUBLESHOOTING CONCEPTS**
- **TROUBLESHOOTING GATES**
- **TROUBLESHOOTING ACCESS ISSUES**
- **TROUBLESHOOTING DOOR ALARMS AND INPUTS**
- **TROUBLESHOOTING COMPUTER ISSUES**
- **TROUBLESHOOTING NETWORK ISSUES**

This chapter covers basic troubleshooting for the Falcon XT and StorLogix system. It is by no means an exhaustive troubleshooting manual. PTI strongly recommends that all installation, troubleshooting, and service be performed by trained and qualified personnel. If help is still required after following the troubleshooting steps in this chapter and having a trained service technician look at the system, contact PTI Technical Support. The most important point about troubleshooting is to follow the setup steps in this manual in order. This will save a lot of time and trouble.

Troubleshooting Concepts



Troubleshooting, like detective work, involves taking a set of clues or symptoms and following them back to a logical conclusion. This can be very difficult if the troubleshooter skips steps or assumes answers. It is very important to be careful, methodical, and thorough when troubleshooting. Follow the steps below in order to help begin the troubleshooting process. It is a good idea to keep a set of notes throughout the process of what steps have been taken and what results have been seen. Be detailed, writing down system messages, error messages, multimeter readings, AI Device addresses, AI Device functions and locations, etc.

The best place to begin troubleshooting is to have a good installer/service company do the install and to have a really good set of records about the system that include: a site map showing the location of all equipment and wiring, a list of AI Devices with functions and locations, regular backups of data from all software, copies of all manuals, all discs for any software, and contact information for the installer and responsible personnel.

1. Begin by asking the question: “Was the item working in the past or has the problem been there since the beginning?” It is important to be very honest at this point. Generally, if something has been installed for awhile, it has probably worked at some point. The trick is to find out when it stopped working and why.
2. If the item is newly installed, and the problem has been present since the beginning, carefully go back over every part of the installation. Refer to the following sections for troubleshooting specific items.

3. Next, ask the question: “What has changed at this site that may have caused the problem?”

Examples include:

- Construction/electrical work on-site or in the area
- Change made to system
- New computer or peripheral added (PDA, printer, hard drive, etc)
- New employee operating system
- Furniture moved (pinching wires/pulling wires)
- Power interruptions or surges (Blackouts or brownouts)
- Lightning strikes or electrical storms
- Vandalism or other physical damage

4. Ask other pertinent questions:

Examples include:

- Was the system working previously?
- When did the problem first occur?
- When and how did the problem first get noticed?
- What was happening immediately before the problem occurred?
- How often does the problem occur?
- Does it tend to occur at certain times or in certain areas?
- Does the problem affect everyone or just certain individuals?

5. Check all wires and cables in the vicinity of the system. Verify that all cables are actually plugged in, that all connections are tight, and that no wires are pinched, crushed, or cut.
6. Try a simple system reset. Locate the Falcon XT controller and press the reset button in the upper left of the circuit board. Hold this reset button in for at least 60 seconds. Larger sites with more AI Devices may require the button to be held in for a longer time to be sure that every AI Device is reset. Once the button is released, watch the StorLogix event log to verify that each device comes back on-line in numeric order by address.
7. Verify that the system is working and that all AI Devices are functioning correctly. If the problem has gone away, monitor the situation for the next few days. If the problem repeats, repeat these steps and compare notes to watch for a pattern. If the problem persists, try the troubleshooting steps on the following pages. After taking these steps, contact PTI Technical Support.

Troubleshooting Gates

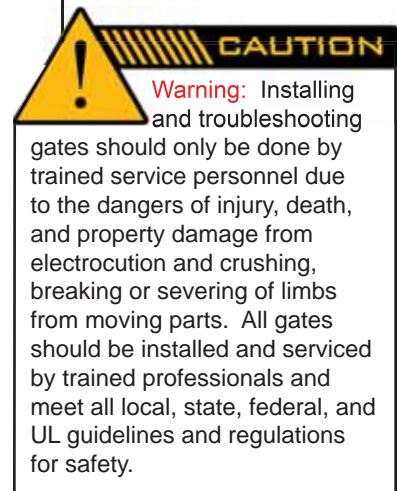


Warning: Installing and troubleshooting gates should only be done by trained service personnel due to the dangers of injury, death, and property damage from electrocution and crushing, breaking or severing of limbs from moving parts. All gates should be installed and serviced by trained professionals and meet all local, state, federal, and UL guidelines and regulations for safety.



1. Most gate problems are due to a lack of maintenance or improper maintenance. Gates should be regularly serviced by a trained service person. A regular routine of service and maintenance should be planned for in the budget and scheduled throughout the years.
 - Gates must be oiled and greased with the recommended lubricants.
 - Parts must be cleaned with the proper solvents.
 - Wheels, gears, chains and other moving parts must be inspected for wear or damage and replaced immediately if necessary.
 - The chain must be tightened and adjusted regularly.
 - Weeds and rocks must be kept away from the chain and gate path.
 - Track must be unbroken, not lifting up or bending, and free from debris.
 - The set screws and adjustment nut must be checked regularly.
 - Loops, beams, and sensor edges should be tested regularly and immediately replaced or repaired if not working correctly.
 - Keep children and pets away from the gate to prevent injury or death. Also, tools, toys, and other items can block the gate opening and closing or cause the gate to go off its track.

2. If there is a problem with the Gate opening or closing, try a code at or card at the AI Device controlling the gate to see what happens. Be sure that the code or card is one that is known to be working.
- If the gate closes on vehicles or people, immediately open the gate using a manual override or block access to the gate to prevent property damage, injury, or death. Then contact a gate service company to come and repair the gate.
 - If the gate does not open at all, refer to the Troubleshooting guidelines for Access Devices on the following pages.
 - If the gate stays partway open or closed, contact a gate service company to send a technician out to service the gate.
 - If the gate is slow, sticking, or hesitating, contact a gate service company to send a technician out to service the gate.
 - If the gate opens and stays open, check the relay settings in StorLogix, the hold open times in StorLogix and in some keypad types, or contact the gate installer to make sure that the safety features aren't holding it.



Troubleshooting Access Issues



REMEMBER

It is a good idea to keep a map of the site, showing the locations of all devices, wiring, and junction boxes.

Use the following troubleshooting steps for access devices including VP keypads, Apex keypads, and Wiegand devices. Remember to keep a good set of notes as you troubleshoot. This can help to compare to find problems, prevent confusion, and help speed things up if site service by a technician or telephone technical support is required.

1. Try a code or card at the AI Device controlling the gate to see what happens. Be sure that the code or card is one that is known to be working at that location and time. It is a good idea to try several codes. Note which code was tried and what the message response at the device is as well as the message response on the StorLogix event log. Check the event against the StorLogix Event Cross-reference in the StorLogix Help menu.
2. Try the same code(s) or card(s) at other Access Devices on the property. Compare the result with the previous step. Try to narrow down if multiple devices are affected or just one.
3. If it can be narrowed down to one device, it must be determined if the problem is in the device or the location. Make sure to allow for access and exit of customers and then remove the device in question. Switch it with another similar device that has been proven to be working in the previous step. For example, if the entrance keypad isn't working, but the exit one is, then switch these two. Be sure to switch the addresses also. If the problem stays in the same location, it is probably a wiring issue. Contact a service company to come and check the wiring. If the problem follows the device, contact PTI technical support for further troubleshooting instructions.

4. If necessary, the process in the previous step can be performed for an entire site, if there are multiple problems or ongoing issues. This is called a full site reset. Generally, this is a sign of problems in wiring, either from bad splices, pinched or nicked wires, radio frequency interference (RFI), water in conduit, or incorrect wire type. To do this for an entire site, make sure to allow for access and exit of customers and then go to every AI Device on the site, opening the housings and unplugging the power and data terminal blocks. When every device on the site is unplugged, add one device in at a time. Allow that device to function for an hour and then add in the next device in line. Eventually, a device will be added that causes the problem to manifest. Switch this device with one that has been previously added to verify if the problem exists in the location or in the device.
5. Verify that all devices are receiving enough power. Create a voltage map of the site, by sketching out the site with the locations of every AI Device. Use a multimeter to take DC power readings at each device. Note these readings on the sketch. Any device that is receiving less than 12 volts is underpowered and can cause the entire system to lock up.
6. Verify that the AI Devices have each been setup in the StorLogix Setup screen, AI Device Properties wizard.
7. Verify that the RS485 LED's (lights) on the Falcon XT board are both blinking constantly. If the red one is not blinking, then there is a break in the communications + wire or no devices are communicating at all. If the green light is not blinking, then the communications - is not working.]
8. If all setup is correct and clients are still getting denied access, select Database Troubleshooter in the Tools drop down menu on the StorLogix Menu bar. Click on the Reference ID Fix button. Then go back and try a code again.

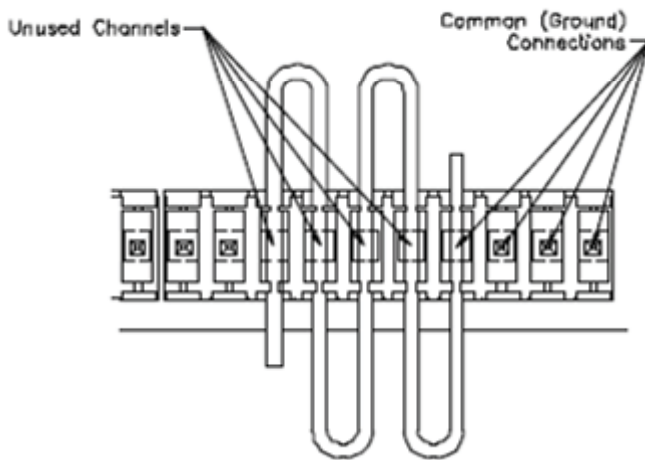
Troubleshooting Door Alarms & Inputs



The following steps can be used for troubleshooting door alarms. Remember to keep a good set of notes as you troubleshoot. This can help to compare to find problems, prevent confusion, and help speed things up if site service by a technician or telephone technical support is required. Many door issues will need to be checked by a trained service technician.

1. Ask the following questions: “Is the problem with a single door (or alarm input) or is it with a bank of doors?” and “Are the units rented or not?” If the unit or units are rented, it may be necessary to gain access to the doors from the tenants for troubleshooting.
2. Check the doors in question. Are they loose, possibly moving due to wind or vibration from traffic?
3. Check each multiplexer on the site. The circuit boards, cases, and wiring should be checked for obvious damage (i.e. vandalism, burn marks from power surge/lightning, corrosion on the circuit board, water marks, insects, construction debris, etc).
4. Check the Voltage across the common and channel input points in the multiplexer that correspond to the door in question. Note: All channels in the multiplexer should be checked as problems with one door or wiring may affect the entire board. Also, all multiplexers on the site should be checked also as problems with one may cause problems in another.
 - Voltage with the door closed should be 0 VDC.
 - Voltage with the door open should be 4.5 – 5 VDC.
 - In case of incorrect readings, remove the punch-terminal block and reverify incorrect readings at the pins to identify if the problem is just an improperly punched wire. If so, repunch the wire using a PTI Multiplexer punch-down tool (PTI Part # TMUX-PD TOOL). Do not use screwdrivers, knives, or other phone system punch-down tools as they will not seat the wire correctly.
 - Any other incorrect readings indicate a short in the door contact wiring, loose connection, or ground loop that needs to be investigated and fixed. This may involve rewiring or replacing a door switch.

5. If the problem is occurring in channels that are not used, tie down all unused channels to Common (Ground). See drawing below. Using a PTI Punch-down tool, punch down a 24 AWG insulated solid wire through any unused door alarm channels and at least one common (ground) connection. Then connect a length of 24 AWG wire from pin # 5 of the power and data terminal block to one of the four screws that mount the circuit board to the metal case. The metal case of the multiplexer must also be mounted directly to a grounded metal building or tied to a ground rod or grounded metal structural element of the building such as a metal water pipe or ground rod in accordance with local code. If at all possible both ends of the shield/ground wire should be tied to ground.



6. Verify that all wire used during installation of the system is correct to PTI specifications. 18 AWG shielded wire should be used for power and communications. 24 AWG telephone wire should be used for the door alarms. Verify that there are no breaks in the shield, skinned or bare wire, shorts or breaks in the wire, and that there are no splices in the wiring other than those required for the door alarm switches.

7. Radio Frequency Interference (RFI) may also be a problem in very rare cases. All electronic equipment is susceptible to radio frequency interference (RFI). PTI manufactured equipment has protection built into it to keep it safe from most RF interference, however, extreme levels of this type of interference can cause communications problems. Radio antennas, military bases, airports, radar, power plants, certain types of lighting and communications equipment, are all examples RF generators that can cause these types of problems. Humidity, temperature, and cloud cover as well as broadcasting strength and proximity to the RF source can all make the problem worse. Generally, extreme levels of RF will cause the PTI system data communications to go on and off (data comm on / data comm off) or cause the system to report scattered false door activity during the times when the RF levels are at the highest. In these extreme cases, Braided Shielded telephone wire and/or RF filters on the door alarm wires may be required in addition to the recommended fixes above. Both of these products are available through PTI and can be installed by a PTI Certified Installer.
8. If necessary, a full site reset can be performed if there are multiple problems or ongoing issues. Generally, this is a sign of problems in wiring, either from bad splices, pinched or nicked wires, radio-frequency interference, water in conduit, or incorrect wire type. To do this for an entire site, go to every multiplexer and AI Device with door alarm inputs on the site, opening the housings and unplugging the power and data terminal blocks. When every device on the site is unplugged, add one device in at a time. Allow that device to function for an hour and then add in the next device in line. Eventually, a device will be added that causes the problem to manifest. Switch this device with one that has been previously added to verify if the problem exists in the location or in the device.
9. Verify that the multiplexer is setup in the AI Device Properties wizard on the Setup screen in StorLogix. Verify also that the inputs are setup in the Inputs wizard and the Inputs to Units wizard on the StorLogix Setup screen.
10. Contact PTI Technical Support if the above steps do not fix the problem for further troubleshooting steps.

Troubleshooting Computer Issues

- Many computer problems can be traced back to some basic issues:
- Make sure that the computer meets or exceeds the computer requirements in Chapter 1. A second-rate computer will give second-rate performance.
- Be sure that the computer is setup by a trained computer professional
- Be sure that all necessary Windows updates have been performed.
- Any new software is added to the computer can interfere with existing programs including StorLogix. Common problems include PDA's, Cell phones, Video games, Cameras, USB Devices, Firewall software, and any program that controls comm ports on the computer.
- Many viruses can cause problems with computer functionality. A good Anti-Virus software is a must.
- Music, Picture, Video, and Game downloads can use up a lot of space on a computer and can slow down performance or interfere with settings that affect the computer functionality.
- Web cookies and spyware from internet usage can slow down the performance of the computer. Not only can these things be annoying, but certain malware types of spyware can be dangerous. A good Anti-Virus and anti-spyware program is recommended. This should be updated regularly. Cookies, Temporary Internet files, and Browser history should be periodically cleared.
- Regular maintenance of the computer by a knowledgeable computer professional will take care of many potential problems before they occur.



REMEMBER

Review the computer requirements in Chapter 1 of this manual. If the computer does not meet these requirements, then this is the place to start troubleshooting.

Troubleshooting Communications

If problems occur with the communication between StorLogix and the Falcon XT, consider the following:


- Be sure the USB cable, RS232 cable, or TCP/IP Ethernet cable is connected from the computer to the Falcon XT board (depending on which one is being used).
- If using the USB connection, the USB cable should have been plugged into the computer before the initial install. If it wasn't, use the StorLogix Install disk to install the USB drivers. Do NOT use Windows updates to install the drivers.
- If the USB drivers are installed but do not appear in the LogixServer setup wizard, step 3, make sure that the USB cable is plugged in and then restart the computer. If this doesn't work, reinstall the USB drivers from the StorLogix Install disk.
- If the USB is unplugged while LogixServer is running, LogixServer will need to be closed and restarted with the USB plugged in. Select the Setup Wizard under Setup in the LogixServer menu bar and make sure that the USB drivers are selected in Step 3. The computer may need to be restarted.
- USB drivers may need to be pointed to C:\Cygna\CP2101\Win. This is done in the Setup Wizard under Setup in the LogixServer menubar. Make sure that the USB drivers are selected in Step 3.
- Check the Falcon XT board. Near the lower center of the board is a LED marked USB. If this light is lit, then the computer port is not working (or the Serial Port or TCP/IP connection is being used).
- If using the RS232 Serial port for the connection, then be sure that the LED's marked RS232 near the lower center of the board are flashing. If not, then communications are not working.
- Try clicking on the Send All to Falcon XT icon on the StorLogix Tools menu.



CAUTION

The USB drivers that are included with StorLogix must be used if the connection between StorLogix and the Falcon XT is made using a USB cable.

These USB drivers must be installed from the StorLogix installation disk. Do NOT use the drivers that are available on the internet for this as they are not the same.



REMEMBER

Note: If using RS232 Serial port communications between the Falcon XT and StorLogix, you must use the cable and connectors provided by PTI. The connectors are specific to the device. Be sure the connector marked PC is connected to the computer and the connector marked Controller is connected to the Falcon XT.

Troubleshooting Networking Issues

Network issues can be very difficult to troubleshoot. All network setup and troubleshooting should be done by a trained IT professional. This is not a task that should be attempted by an untrained person.

Below are some common issues to consider:

- When trying to connect to a different database, if the other database doesn't show, then the database may not be on this network. The Server Network Utility may not have been correctly completed.
- If the TCP/IP LED's on the Falcon XT board are not blinking then no communications are occurring.
- If unable to connect to the DVR. The wrong IP, username, or password may have been entered into StorLogix DVR setup or the DVR may not be on the network.
- Port forwarding may not have been setup if using a router.
- Software Firewall or Anti-Virus software may be interfering with network access.
- Verify that the ethernet cable is connected and that the connection is correctly made. Try switching with another ethernet cable or connection port.
- Verify that the modem or router is connected and has power and is actually working.
- Verify that the internet connection is up and running. In most cases, the connection must have a static IP and always be on. The internet connection must be high-speed.
- Verify that StorLogix has been setup and is working on each computer on the network and that it is pointed to the correct computer name with the database on it.
- If using wireless networks, verify that encryption is not on one end but not the other. The computer must have the proper encryption key.



??????? HINT

Try accessing the internet from the computer. If the browser is unable to access the internet, then that could be a sign that the network is not setup correctly or there are problems with the router, modem, or internet connection.

If the internet connection is working, then make sure that StorLogix and LogixServer are correctly setup.

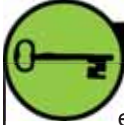
CHAPTER 12: APPENDIX

- **FALCON 2000 TO FALCON XT FUNCTION CROSS-REFERENCE**
- **NOTICES, WARNINGS, AND DECLARATIONS**
- **EULA**
- **STANDARD 2-YEAR EQUIPMENT WARRANTY**
- **CONTACT PTI**
- **GLOSSARY**
- **INDEX**

The Appendix contains common reference information for StorLogix, PTI, and PTI equipment.

Falcon 2000 to Falcon XT Cross Reference

Falcon Base Unit	F2K Function
Falcon Base Unit	
	Falcon 2000
Remote (or Remote Device)	
Function 1 - Set Time & Date	Manual Operations Icon - Set Date and Time
Function 2 - Set Time Zones - Days	Site Setup Icon - Time Zone Setup - Hours
Function 2 - Set Time Zones - Keypads	Site Setup Icon - Time Zone Setup Allowed Remotes
Function 3 - Set Holidays	Site Setup Icon - Holiday Setup
Function 4: Vacate a Unit	Units Icon - Vacate Unit
Function 5: Rent a Unit	Units Icon - Rent Unit
Function 5: Section Number	
Function 5: Unit Number	
Function 5: Code	
Function 5: Expiration Date	
Function 5: Zone	
Function 5: Alarm Mux	Protected Site Setup - Mux and Channel Assignment
Function 5: Channel	Protected Site Setup - Mux and Channel Assignment
Function 5: Unit Alarm On/Off	Protected Site Setup - Unit Alarm Control
Function 5: Unit Lockout Off/On	Units Icon - Suspend Access Units Icon - Un-Suspend Access
Function 6: Delete a Unit	
Function 7: Set Contrast Code	Protected Site Setup - Falcon Setup - Contrast Adjust Code
Function 8: Print Reports	Reports Icon
Function 8: All Units Report	Reports Icon - All Units
Function 8: Suspended Units Report	Reports Icon - Suspended Tenants
Function 8: Vacant Units Report	Reports Icon - Vacant Units
Function 8: Open Units Report	Reports Icon - Open Units
Function 8: On-site Units Report	Reports Icon - On-site Tenants
Function 8: System Setup Report	Site Setup Icon - Print System Setup
Function 8: Status Report	Reports Icon - Remote Online Status
Function 8: Cancel Report	
Function 9: Save to Tape	
Function 10: Load from Tape	
Function 11: Open Entrance	Manual Operations Icon - Trigger Relay
Function 12: Clear Alarms	Manual Operations Icon - Clear Alarms



???????? HINT

Dealers, installers, and end users that have used the PTI Falcon Base Unit and Falcon 2000 access control system in the past, will find that the Falcon XT and StorLogix access control system has more functions and abilities than the previous product.

It is important to note, however, that almost every function that was in the old Falcon system can be found in the new Falcon XT and StorLogix system.

The chart on the following pages is a cross-reference tool to assist you in finding the equivalent new function in StorLogix that you may have used in the Falcon and Falcon 2000.

Falcon XT/StorLogix Equivalent	
	Falcon XT
	StorLogix
	AI Device
	Tools screen - Synchronize Date/Time
	Setup screen - 3. Time Schedules (to create hours) Setup screen - 12. Access Levels (to combine Time Schedules and Access Areas)
	Setup screen - 11. Access Areas (to create areas) (to create hours) Setup screen - 12. Access Levels (to combine Time Schedules and Access Areas)
	Setup screen - 19. Holidays
	User Operations screen - Vacate Unit
	User Operations screen - Rent Unit
	Setup screen - 9. Buildings (to setup Building) Setup screen - 11. Access areas (to add units)
	Setup screen - 14. Units
	Menu Bar - Edit - Cards - Setup Cards/Codes (to add codes to the system) User Operations - Rent Unit or Edit User step 2 (to assign code to user)
	Menu Bar - Edit - Cards - Setup Cards/Codes step 2 (to add start and end date to the card) User Operations - Rent Unit or Edit User step 2 (to add expiration date to code/card for a user)
	Rent Unit step 4 to set Access Level or Edit User step 4 to set Access Level or Add User step 3 to set Access Level
	Setup screen - 15. Inputs to Units to create or import Alarm file.
	Setup screen - 15. Inputs to Units to create or import Alarm file.
	User Operations screen - Edit Unit step 3 Door Alarm Active
	User Operations screen - Suspend Unit OR Suspend User
	Setup Screen - 14. Units step 1 select the unit and click remove
	Setup Screen - 17. Falcon XT - step 3 Contrast Code
	Menu Bar - Reports - Launch ReportViewer
	Reports - All Units
	Reports - Suspended Units
	Reports - Vacant Units
	Reports - Open Units
	Reports - On-site Users
	Reports - Any report that ends in 'Configuration'
	Reports - AI Device Status
	N/A
	N/A
	N/A
	User Operations Screen - Open Door/Gate
	Menu Bar - Tools - Clear All Alarms

Falcon 2000 to Falcon XT Cross Reference

Falcon Base Unit	F2K Function
Function 13: Alarm Controls	Protected Site Setup - Falcon Setup - Alarm Controls
Function 13: Alarm System On/Off	Protected Site Setup - Falcon Setup - All Alarms
Function 13: Vacant Alarms On/Off	Protected Site Setup - Falcon Setup - Vacant Alarms
Function 13: Rem Comm Alarms On/Off	Protected Site Setup - Falcon Setup - Communications Alarms
Function 13: Tamper Alarms On/Off	Protected Site Setup - Falcon Setup - Tamper Alarm
Function 13: Unknown Channels On/Off	Protected Site Setup - Falcon Setup Unknown Door Alarms
Function 13: Auxillary Sirens On/Off	Protected Site Setup - Falcon Setup - Aux Siren
Function 13: Day Siren =	Protected Site Setup - Falcon Setup - Alarm Time (Day)
Function 13: Nite Siren =	Protected Site Setup - Falcon Setup - Alarm Time (Night)
Function 13: Rearm Time	Protected Site Setup - Falcon Setup - Alarm Rearm
Function 14: Control Options	
Function 14: Printer Logging	
Function 14: Relay Time	
Function 14: Max Remotes	Protected Site Setup - Falcon Setup - Number of Remotes
Function 14: RS232 Baud	
Function 14: RS485 Baud	Protected Site Setup - Falcon Setup - RS485 Baud Rate
Function 15: Adjust Contrast (On Falcon Base Unit Display)	
Function 16: Update Graphics	Manual Operations Icon - Update Graphics
Function 17: Program Version	
Function 18: Setup Remotes	Protected Site Setup - Remote Station Setup
Function 19: Setup Elevators	Protected Site Setup - Elevator Setup
Function 20: Setup Lighting Zones	Protected Site Setup - Lighting Setup
Function 21: Clear Remotes	
Function 22: Clear Elevators	
Function 23: Clear Lighting Zones	
Function 24: Clear On-site Users	Manual Operations Icon - Clear Users On-site
Function 1000: Factory Setup	
Function 1000: Change Password	
Function 1000: Firmware Reprogram Off/On	
Function 1000: Alarms Enable	
Function 1000: Graphics Enable	
Function 1000: Modem Enable	
Function 1000: Section Letters	
Function 1000: European Dates	

	Falcon XT/StorLogix Equivalent
	Primarily found in Setup Screen - 17. Falcon XT step 2
	Setup Screen - 17. Falcon XT step 2 - Entire Alarm System ON
	Setup Screen - 17. Falcon XT step 2 - Vacant Alarms On
	Setup Screen - 17. Falcon XT step 2 - Communication Alarms On
	N/A
	Setup Screen - 17. Falcon XT step 2 - Undefined Input Reporting
	Setup Screen - 17. Falcon XT step 1 Auxillary Sirens Alarm Zone.
	Setup Screen - 7. Alarm Zones step 2 Day Mode
	Setup Screen - 7. Alarm Zones step 2 Night Mode
	Setup Screen - 14. Units step 2 Rearm (for unit alarms) OR Setup Screen - 11. Access Areas step 2 Rearm Wait Time (for area alarms)
	N/A
	N/A
	Setup Screen - 5. Relays step 2 - Activate Time
	Setup Screen - 17. Falcon XT step 3 - Maximum AI Device Address
	LogixServer setup wizard step 3. Right-click on LogixServer in the taskbar on the start bar. Select LogixServer Setup Wizard.
	Setup Screen - 17 Falcon XT step 1 - AI Devices Baud Rate
	N/A
	Tools screen - Update Graphics
	Menu Bar - Help - About StorLogix - Falcon XT v
	Setup Screen - 4. Enroll AI Devices AND 16. AI Device Properties
	Setup Screen - 10. Elevators
	Setup Screen - 8. Lighting Areas
	Setup Screen - 4. Enroll AI Devices AND 16. AI Device Properties - remove AI Device
	Setup Screen - 10. Elevators - Remove
	Setup Screen - 8. Lighting Areas - Remove
	Menu Bar - Tools - Clear All On-Site Users
	Setup Screen
	N/A - however, you can setup security levels in Setup Screen - 2. Security Levels to keep operators out of this area.
	N/A
	Setup Screen - 17. Falcon XT step 2 - Entire Alarm System ON
	Setup Screen - 17. Falcon XT step 2 - Site Graphics
	N/A
	N/A
	N/A (Setup in the Keypads individually - StorLogix has European dates only if the Window's Operating System is setup that way)

Falcon 2000 to Falcon XT Cross Reference

Falcon Base Unit	F2K Function
Function 1000: Free Exit	
Function 1000: Anti-Passback	
Function 1000: Lighting Controls On/Off	
Function 1000: Count Users	
Function 1000: CheckIn Pad <=	
Function 1000: Exempt Zone >=	
Function 1000: Counter Rdr =	
Function 1000: Comm Count	
Function 1000: Midnight Log Out	
Function 1000: Swinger Shutdown	
Function 1000: Ignore OS Doors	
Function 1000: Daily Status Rpt	
Function 1000: Limit Code Size	
Function 1000: Trig. Mux	
Function 1000: Trig. Ch	
Function 1000: Reset Mux	
Function 1000: Rst Ch	
Function 1000: Gate Mux	
Function 1000: Gate Ch	
Function 1000: Enter unit # for Relay	
Function 1000: Enter relay # to Trip	
Function 1001:	
Function 1002: Loopback Test	
Function 1003: Erase All User Data	
	Units Icon - Transfer Unit
	Units Icon - Copy Unit
	Units Icon - Edit Unit
	Units Icon - Edit Unit Size and Price
	Units Icon - Edit Tenant
	Backup / Restore Icon - Backup Customer Data
	Backup / Restore Icon - Backup Falcon Settings
	Backup / Restore Icon - Restore Customer Data
	Backup / Restore Icon - Restore Falcon Settings
	Reports Icon - Today's Site Activity
	Reports Icon - Unit Activity By Unit Number

Falcon XT/StorLogix Equivalent
Setup Screen - 17. Falcon XT - step 4 Late Exit Mode, Late Exit Grace Period, and Late Exit Count Limit.
Setup Screen - 17. Falcon XT - step 4 Anti-passback mode and Anti-passback Time
N/A
Setup Screen - 16. AI Device Properties step 5 - Clear User On-site Count When Exiting.
Setup Screen - 16. AI Device Properties step 3 - AI Device Function mode to make a device a check-in pad. Same wizard, step 2 for other access devices to require checkin at the checkin pad before being able to use them.
Setup Screen - 12. Access Levels step 3, select all access areas that they are allowed into.
N/A - cards are setup in advance in the Menu Bar - Edit - Cards - Setup Cards wizard.
Setup Screen - 17. Falcon XT step 3 Comm Count. This should always be set between 8 - 12.
Setup Screen - 17. Falcon XT step 1 Log Off Time of Day (it can now be set to any time, not just midnight).
Setup Screen - 6. Inputs - step 3 - Enable Swinger Shutdown, Swinger Time Period, and Swinger Count.
Setup Screen - 6. Inputs - step 3 - Ignore On-Site Activity
N/A
Setup Screen - 17. Falcon XT step 3 - Maximum Code Size
N/A
N/A
N/A
N/A
N/A
N/A
N/A
N/A
N/A
N/A
Menu Bar - File - Clear Controller Database
N/A
N/A
User Operations - Edit Unit
N/A
User Operations - Edit User
Menu Bar - File - Backup
Menu Bar - File - Backup
Menu Bar - File - Restore
Menu Bar - File - Restore
Reports - Site Activity by Date
Reports - Unit Activity by Date

Falcon 2000 to Falcon XT Cross Reference

Falcon Base Unit	F2K Function
	Reports Icon - Unit Activity By Unit Number
	Reports Icon - Unit Activity By Name
	Reports Icon - Comm On/Off by Date
	Reports Icon - Current Alarms
	Reports Icon - Historical Alarms By Date
	Reports Icon - Low Battery Report
	Reports Icon - Rented Units
	Reports Icon - Security Levels
	Reports Icon - Security Log
	Reports Icon - Site Activity by Date
	Reports Icon - Site Activity by Remote
	Reports Icon - Site Activity by Time Zone
	Reports Icon - Suspended Tenants w/Address
	Reports Icon - Transmitter Check-In Report
	Reports Icon - Units with Alarms Off
	Reports Icon - Units with Size and Price
	Reports Icon - Users
	Site Setup Icon - Edit Relays to Trigger
	Site Setup Icon - Edit Base Unit Sizes/Prices
	Site Setup Icon - Send All to Falcon
	Site Setup Icon - Retrieve All from Falcon
	Site Setup Icon - Edit Company Settings
	Protected Site Setup - Unit Configuration
	Protected Site Setup - Send Falcon Binary Program
	Protected Site Setup - Archive Data
	Protected Site Setup - Clear All Information
	Protected Site Setup - Print All Units with Passcodes
	Protected Site Setup - Print Internal F2000 Errors
	Protected Site Setup - User Management
	Protected Site Setup - Security Levels
	Menu Bar - File - Print to RTF file
	Menu Bar - File - Import Alarm File
	Menu Bar - Sites - Disconnect
	Menu Bar - Sites - Connect to...
	Menu Bar - Help - Contents and Index
	Menu Bar - Help - What's This?
	Menu Bar - Help - About Falcon 2000

	Falcon XT/StorLogix Equivalent
	Reports - Unit Activity by Date
	Reports - User Activity by Date
	Reports - Communications On/Off
	Reports - Alarms Event
	Reports - Alarms Event
	N/A
	Reports - Rented Units
	N/A
	N/A
	Reports - Site Activity by Date
	Reports - Site Activity by AI Device and Date
	Site Activity by Access Area and Date
	N/A
	N/A
	N/A
	N/A
	N/A
	Setup screen - 5. Relays
	N/A
	Tools Screen - Send All to Falcon XT
	N/A
	LogixServer setup wizard. Right-click on LogixServer in the taskbar on the start bar. Select LogixServer Setup Wizard. Also, Setup Screen - 1. Company Info
	Setup Screen - 14. Units
	LogixServer - Menu Bar - Tools - Update Falcon XT Firmware
	Menu Bar - File - Archive Events
	Menu Bar - File - Clear Falcon XT Database
	N/A
	N/A
	User Operations Screen - Add User
	Setup Screen - 2. Security Levels
	N/A
	Setup Screen - 15. Inputs to Units - Import/Export
	Menu Bar - File - Change Database Connection
	Menu Bar - File - Change Database Connection
	N/A
	N/A
	Menu Bar - Help - About StorLogix

Notices, Warnings, and Declarations



We strongly recommend that installation and setup of any PTI equipment be done by a certified, licensed, qualified, and competent person. PTI Integrated Systems can recommend local dealers and installers, but it is up to the customer to verify their qualifications and negotiate any pricing or contracts unless PTI has been specifically contracted in writing to do so for the customer. With any computer setup or installation, some troubleshooting and adjustment of the configuration may be required. This will differ with every installation and computer setup depending on operating system, software installed on it, quality of components, internet connection, modem connection, and any site-specific variables. This troubleshooting and configuration may include purchasing additional equipment. In no circumstances will PTI Integrated Systems be responsible for any damages either incidental or consequential based on these recommendations. All installation of electronics and electrical systems must be in compliance with local, municipal, state, and the National Electrical Code.

Installation of equipment manufactured by PTI Integrated Systems must be performed per our recommendations and guidelines except where local, municipal, state, provincial, and National Electrical and Construction codes take precedence. When code and our guidelines do not cover a given situation, it is the responsibility of the Dealer/ Installer to contact PTI for instruction and/or follow established custom and best practices applicable to the particular trade. Dealers and Installers must know and abide by all existing laws pertaining to their work.

Reliable equipment operation is dependent upon noise free uninterrupted sources of power. The PTI Falcon battery back-up feature is provided primarily to preserve the integrity of the memory database and operation of the PTI Falcon system. This will not guarantee operation of the gate motor or door actuator for emergency situations in the event of a power loss or equipment failure. It is the sole responsibility of the purchaser to provide for and facilitate manual non-electrical emergency means of exit in the event of a power failure. Contact your local dealer/installer for options and availability.

Notices, Warnings, and Declarations



The User should follow all installation, operation, and maintenance instructions. The User is strongly advised to conduct Product and systems test at least once each week. Changes in environmental conditions, electric or electronic disruptions, and tampering may cause the Product to not perform as expected.

PTI warrants its Product to the User. The User is responsible for exercising all due prudence and taking necessary precautions for the safety and protection of lives and property wherever PTI Products are installed. PTI does not authorize the use of its Products in applications affecting life safety.

Some PTI products use 900Mhz wireless technology. Other devices at the site such as cordless telephones or alarm components may cause interference that will disrupt the operation of the system or may be interfered with by the system. PTI assumes no liability for any problems caused by interference. It is the sole responsibility of the user to identify and correct such problems.

This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with this manual, may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A computing device pursuant to Subpart J of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference in which case the user at his/her own expense will be required to take whatever measures may be required to correct the interference.

This manual and all documentation for PTI products belong to the User and must be given to them by the Dealer or Installer immediately after installation. These items should be retained on-site by the User.



End User License Agreement (EULA)

Important Notice: This Software End User License Agreement (EULA) is a legal agreement between you (either an individual or, if purchased or otherwise acquired by or for an entity, an entity) and PTI Integrated Systems (PTI) for the software product that this EULA is contained on. This includes the software product and any other documentation or media that accompanies it. **READ IT CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AND USING THE SOFTWARE AS IT PROVIDES A LICENSE TO USE THE SOFTWARE AND CONTAINS WARRANTY INFORMATION AND LIABILITY DISCLAIMERS.** In order to use this software, you must first accept the terms of this EULA, and confirm your acceptance of the terms of this EULA by pressing the 'I Agree' button on the PTI download screen. By installing, copying, or otherwise using any portion of this software, you are confirming your acceptance of the software and agreeing to become bound by the terms of this EULA. You agree that this EULA is enforceable like any written negotiated agreement signed by you. If you do not agree to be bound by these terms, then do not install or use the software in anyway; contact PTI immediately to make arrangements to return the product. If you acquired the software on tangible media (e.g. CD) without an opportunity to review this license and you do not accept this agreement, do not use the software, contact PTI immediately within 30 days of purchase or otherwise acquiring of the software to arrange to return the software product. If you press the 'I Don't Agree' button on the software download screen you will not be able to install the software.

1. Definitions

- 1.1. "Use" or "Using" means to access, install, download, copy or otherwise employ the functionality of the Software.
- 1.2. "Computer" means an electronic device that accepts information in digital or similar form and manipulates it for a specific result based on a sequence of instructions.
- 1.3. "Documentation" means any manuals, technical support documents, drawings, diagrams, or help files that accompany this software or can be obtained from PTI regarding this software as of the date of purchase.
- 1.4. "PTI" or "PTI Integrated Systems" means Preferred Technology, Inc. dba PTI Integrated Systems located at 8271 East Gelding Drive in Scottsdale, Arizona 85260 also referred herein as "We", "Our", and "Us".
- 1.5. "User" means the licensed purchaser or their assigned representative also referred herein as "You" or "Your"
- 1.6. "Software" means all of the contents of the files, disk(s), CD-ROM(s) or other media with which this EULA is provided, the PTI software program(s) and third party software programs, in each case, supplied by PTI herewith, and corresponding documentation, associated media, printed materials, and online or electronic documentation, and all updates or upgrades of the above that are provided to you including any and all additions, copies, modules, versions, variations, revisions, modifications, updates, or upgrades of the program(s).
- 1.7. "Module" means any optional software additions, functions, or components that are not normally included in the base purchase price, but may be added at purchase or at a later date by paying an additional fee.

2. Grant of License

- 2.1. Subject to your compliance with all the terms of this EULA and the purchase of the software from PTI, PTI grants you one single, limited, non-exclusive, personal, non-sublicensable, non-assignable licence to install and use the PTI software herewith on a computer in accordance with the purposes and functionality described in the documentation and only in accordance with this EULA.
- 2.2. The Software is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties.
- 2.3. The Software is licensed, not sold, to you by PTI upon purchase from PTI. The License gives you limited rights to use the Software. You do not become the owner of the software. PTI retains title to the software, and all copies thereof.
- 2.4. All rights not specifically granted in this License, including International Copyrights, are reserved by PTI.
- 2.5. The Software in this package and any copies which this License authorizes you to make are subject to this License.
- 2.6. This EULA covers a single copy of the software program. You must purchase additional licenses if you intend to use multiple copies of this software.
- 2.7. You may install and use the Software on a single desktop computer that has a Windows PC operating system that meets our computer recommendations including desktop PC versions of Windows 98 2nd Edition, 2000 Professional, NT, and XP Professional provided, however, that, notwithstanding anything contrary contained herein, you may not use the Software on any non-PC product or any embedded or device versions of the above operating systems, including, but not limited to, mobile devices, internet appliances, set top boxes (STB), handhelds, PDAs, phones, web pads, tablets, game consoles, TVs, DVDs, gaming machines, home automation systems, kiosks or any other consumer electronics devices or mobile/cable/satellite/television or closed system based service.
- 2.8. A license for the Software may not be shared, installed or used concurrently on different computers.

- 2.9. If the software is loaded on a network, then each person accessing the Software through the network must have a copy licensed to that person
- 2.10. You may make one backup copy of the Software in machine-readable form solely for backup purposes, provided your backup copy is not installed or used on any computer. You must reproduce on any such copy all copyright notices and any other proprietary legends found on the original. You may not transfer the rights to a backup copy unless you transfer all rights in the Software as provided under the Transfer section contained herein.
- 2.11. A license for the software product may not be shared or used concurrently on different computers.
- 2.12. In addition to the single license permitted under this section, a current PTI authorized dealer may make one (1) copy of the software with the user's permission for the dealer's exclusive use on either a portable computer or a computer located at the dealer's business address, provided the software on the portable or home computer is not used for any other purpose than initial setup of the user's single license under this section or to service and troubleshoot the user's single license under this section. The PTI authorized dealer may NOT maintain more than one single copy of any software sold by PTI unless the dealer purchases other licenses. The PTI authorized dealer is also bound by this EULA with regard to the copy they maintain. Dealers who are not currently authorized by PTI or are put on 'inactive status' by PTI are not eligible for this.
- 2.13. PTI software may be made available for a 30-day demonstration period for the purpose evaluating whether to purchase a license to the commercial version of the program. During this demonstration period, you may receive sales related demonstration assistance, but you are not entitled to full business support, hard-copy documentation, or other full access assistance which is available after the purchase of the product.
- 2.14. Beta Testing - In some cases PTI software is made available under pre-commercial release beta testing terms. If the product you have received with this license is pre-commercial release or beta software, then the following Section applies.
 - 2.14.1. To the extent that any provision in this Section is in conflict with any other term or condition in this EULA, this Section shall supercede such other term(s) and condition(s) with respect to the pre-release software, but only to the extent necessary to resolve the conflict.
 - 2.14.2. You acknowledge that the software is a pre-release version, does not represent final product from PTI, and may contain bugs, errors and other problems that could cause system or other failures and data loss. Consequently, the pre-release software is provided to you "AS-IS", and PTI disclaims any warranty or liability obligations to you of any kind. WHERE LIABILITY CANNOT BE EXCLUDED FOR PRE-RELEASE SOFTWARE, BUT IT MAY BE LIMITED, PTI'S LIABILITY AND THAT OF ITS SUPPLIERS SHALL BE LIMITED TO THE SUM OF FIFTY DOLLARS (U.S. \$50) IN TOTAL.
 - 2.14.3. You acknowledge that PTI has not promised or guaranteed to you that pre-release software will be announced or made available to anyone in the future, PTI has no express or implied obligation to you to announce or introduce the pre-release software and that PTI may not introduce a product similar to or compatible with the pre-release software. Accordingly, you acknowledge that any research or development that you perform regarding the pre-release software or any product associated with the pre-release software is done entirely at your own risk.
 - 2.14.4. During the term of this EULA, if requested by PTI, you will provide feedback to PTI regarding testing and use of the pre-release software, including error or bug reports.
 - 2.14.5. If you have been provided the pre-release software pursuant to a separate written agreement, your use of the software is also governed by such agreement. You agree that you may not and certify that you will not sublicense, lease, loan, rent, assign or transfer the pre-release software. Upon receipt of a later unreleased version of the pre-release software or release by PTI of a publicly released commercial version of the software, whether as a stand-alone product or as part of a larger product, you agree to return or destroy all earlier pre-release software received from PTI and to abide by the terms of this EULA for any such later versions of the pre-release software. Notwithstanding anything in this Section to the contrary, if you are located outside the United States of America, you agree that you will return or destroy all unreleased versions of the pre-release software within thirty (30) days of the completion of your testing of the software when such date is earlier than the date for PTI's first commercial shipment of the publicly released software.
- 2.15. Modules
 - 2.15.1. Certain optional software additions, functions, upgrades and/or components that are not normally included in the base purchase price, may be added at purchase or at a later date by paying an additional fee.
 - 2.15.2. Non-purchased modules may be visible within the software but non-functional until purchased from and activated by PTI.
 - 2.15.3. You agree not to access or attempt to access these modules without purchasing them from PTI.
 - 2.15.4. Purchase of module(s) does not confer additional license(s) or entitlements. Upon purchase, the module(s) become a part of the software and subject to this EULA.

3. Restrictions & Limitations

- 3.1. All rights to Use the Software are granted on condition that such rights are forfeited if you fail to comply with the terms of this EULA.
- 3.2. Distribution
 - 3.2.1. You agree not to make or distribute copies of the software, or electronically transfer the Software from one computer to another or over a network.
 - 3.2.2. You agree not to sell, rent, lease, lend, sublicense, grant a security interest in or otherwise transfer the rights to the software or remove any proprietary notices on or in the software.
 - 3.2.3. You agree not to use the software to intentionally or unintentionally violate any applicable local, state, national or international law, or any regulations requirements, procedures or policies in force from time to time relating to the software
 - 3.2.4. You may not alter, merge, modify, adapt or translate the Software, or decompile, reverse engineer, disassemble, or otherwise reduce the Software to a human-perceivable form or otherwise attempt to discover the source code of the Software except to the extent you may be expressly permitted to decompile under applicable law.
 - 3.2.4.1. You may not create derivative works based upon the software.
 - 3.2.4.2. You shall not use the Software to develop any software or other technology having the same primary function as the Software, including but not limited to using the Software in any development or test procedure that seeks to develop like software or other technology, or to determine if such software or other technology performs in a similar manner as the software.
 - 3.2.4.3. If it is essential to do so in order to achieve operability of the software with another software program, you must request PTI to provide the information necessary to achieve such operability. PTI has the right to impose reasonable conditions and to request a reasonable fee before providing such information. Any such information supplied by PTI and any information obtained by you by such permitted decompiling may only be used by you for the purpose described herein and may not be disclosed to any third party or used to create any software which is substantially similar to the expression of the software. Requests for information should be directed to the PTI Engineering Department. PTI does not guarantee that such requests will be approved or such information will be provided.
 - 3.2.4.4. You may not include the software (whole or in part) in any commercial package without PTI's written permission. Software may not be distributed for profit in any form, including, but not limited to, electronic information service distribution, bulletin board distribution, user groups, online services, redistribution companies, and magnetic or optical medium distribution, unless explicitly stated in writing and signed by PTI.
 - 3.2.4.5. You may not alter the code for the purpose of redistributing or selling this program as a free or commercial program under another program name or company name.
- 3.2.5. You may not permit other individuals to use the Software except under the terms listed in this EULA.
- 3.2.6. You may not separate the component parts of the software for use on more than one computer.
- 3.2.7. If you receive the software in more than one medium. Regardless of the type or size of medium you receive, you may use only one medium that is appropriate for your single computer. You may not use or install the other medium on another computer. You may not loan, rent, lease, lend or otherwise transfer the other medium to another user, except as part of the permanent transfer of the software product as covered in the Transfer section of this EULA.
- 3.2.8. You shall not copy the software except as set forth in Section 2. Any copy of the software that you make must contain the same copyright and other proprietary notices that appear on or in the software.
- 3.2.9. User Responsibilities
 - 3.2.9.1. Various states and municipalities have specific limitations and requirements for taxes, fees, customer notifications, auction processes, collections procedures, etc. It is the user's sole responsibility to verify the information and conduct their business in compliance with all applicable laws and codes. PTI strongly recommends that the user verify all information in the software that is applicable to their business and make themselves aware of their legal responsibilities, obligations, and limitations with respect to the use of the software.
 - 3.2.9.2. If your national, state, or local laws allow or require rights, liabilities, and warranties that are not expressly a part of this EULA then you are required to take all reasonable measures to avoid and reduce damages, in particular to make back-up copies of the Software and your computer data subject to the provisions of this EULA.

- 3.2.10. The Software may contain third party software which requires notices and/or additional terms and conditions and are made a part of and incorporated by reference into this EULA. By accepting this EULA, you are also accepting the additional terms and conditions, if any, set forth therein.
- 3.2.11. Any other party using this software must comply with this EULA.
- 3.2.12. The registered licensed end user of this software is ultimately responsible for compliance with all aspects of this EULA.

4. Ownership & Title

- 4.1. The structure, organization and code of the Software are the valuable trade secrets and confidential information of PTI. The Software is protected by law, including without limitation the copyright laws of the United States and other countries, and by international treaty provisions as well as other intellectual property laws and treaties. Except as expressly stated herein, this EULA does not grant you any intellectual property rights in the software and all rights not expressly granted are reserved by PTI.
- 4.2. Intellectual Rights
 - 4.2.1. Logos, Trademarks, code, Product Names, belong to us
 - 4.2.1.1. PTI logos, product names, source code, software structure and organization copyrights, and trademarks contained in the Software are the property of Preferred Technology, Inc. dba PTI Integrated Systems. Third party trademarks, trade names, product names and logos may be the trademarks or registered trademarks of their respective owners. You may not remove or alter any trademark, trade names, product names, logo, copyright or other proprietary notices, legends, symbols or labels in the software. This EULA does not authorize you to use PTI's or its licensors' names or any of their respective trademarks.
 - 4.2.1.2. All images, photographs, animations, video, audio, music, text, and "applets" incorporated into the software, the accompanying printed materials, and any copies of the software are owned by PTI. This EULA grants you no rights to use such content. All rights not expressly granted are reserved by PTI.
 - 4.2.1.3. No rights or licenses are granted by PTI under this EULA, expressly or by implication, with respect to any proprietary information or patent, copyright, trade secret or other intellectual property right owned or controlled by PTI, except as expressly provided in this License.
 - 4.3. Transfer of Software and License
 - 4.3.1. The initial user of the software may make a one-time permanent transfer of this EULA and software only directly to an end user. This transfer must include all copies of the software, backups, documentation, component parts, the media and printed materials, any upgrades, and this EULA. Such transfer may not be by way of consignment or any other indirect transfer. The transferee of such one-time transfer must agree to comply with all of the terms of this EULA, including the obligation not to further transfer this EULA and software.
 - 4.3.2. In event of such transfer, you must inform PTI in writing within 30 days with all information about the previous licensee the new licensee (including, business name, contact person, business address, business phone number, and the reason for transfer).
 - 4.3.3. PTI charges a fee for this transfer that must be paid prior to the transfer. You must contact PTI to make arrangements to pay this transfer fee.
 - 4.3.4. Software may not be transferred to another person if it has not been paid for.
 - 4.3.5. Software transfer does not convey support subscription or future upgrades to the new licensee. Support subscription plan and future upgrades must be purchased by the new licensee.
 - 4.3.6. All backups, loaded software, and other electronic versions of the software must be deleted or uninstalled from the previous licensee's computer.
 - 4.3.7. Upon such transfer meeting these requirements, your license is then terminated and all of your rights in this EULA are transferred to the new licensee. All obligations required to protect PTI are still applicable after the transfer of license.
 - 4.4. Export Rules
 - 4.4.1. None of the Software or underlying information or technology may be downloaded or otherwise exported or re-exported into any country prohibited by the United States Export Administration Act; to a national or resident of Cuba, Iran, Iraq, Libya, North Korea, Sudan, Syria, Yugoslavia or any other country to which the U.S. has embargoed goods who intends to transmit or transport the products back to such country; or to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Denial Orders. By downloading or using the Software, you are agreeing to the foregoing and you are representing and warranting that you are not located in, under the control of, or a national or resident of any such country or on any such list.

5. License Compliance

- 5.1. You agree that PTI or our authorized representative may audit your use of the software for compliance with these terms at any time, upon reasonable notice of 30 days.
- 5.2. In the event that such audit reveals any use of the software by you other than in full compliance with the terms of this EULA, you shall reimburse PTI for all reasonable expenses related to such audit in addition to any other liabilities you may incur as a result of such non-compliance.

- 5.3. Should legal action or arbitration be undertaken to enforce your compliance with this EULA, you agree to pay all court or arbitration costs, reasonable attorney fees, fines and punitive damages that arise there from for yourself and for PTI.

6. Warranty

6.1. Limited Warranty

- 6.1.1. PTI warrants that the software will perform substantially in accordance with the accompanying written materials for a period of one year from the date of receipt if installed and used as directed by PTI, and that PTI technical support will make commercially reasonable efforts to solve any problem.
- 6.1.2. If applicable law requires any other warranties or implied warranties with respect to the software, all such warranties are limited in duration to ninety (90) days from the date of delivery. Some states/jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

6.2. Warranty Disclaimer

6.2.1. As-is

- 6.2.1.1. You expressly acknowledge and agree that use of the Software is at your sole risk. e software is provided "AS IS", and on an "AS AVAILABLE" basis and other than the above limited warranty, there are no claims, representations and warranties made by PTI, either express, implied or statutory (to the extent permitted by applicable law), with respect to the software, including but not limited to, warranties of quality, performance, title, non-infringement, merchantability or fitness for a particular purpose, nor are there any warranties created by course of dealing, course of performance or trade usage.
- 6.2.1.2. Any data downloaded through the use of the software or from any PTI source (including but not limited to the PTI website, PTI FTP site, pcAnywhere®, or Windows XP® connection by PTI) is done at your own discretion and risk (even if recommended by a PTI employee or representative) and you will be solely responsible for any damages to your computer system or loss of data that results from the download or use of any such material.
- 6.2.1.3. The software is not designed, intended or licensed for use in Life Safety or hazardous environments requiring fail-safe controls, including without limitation, the design, construction, maintenance or operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, and life support or weapons systems. PTI specifically disclaims any express or implied warranty of fitness for such purposes.
- 6.2.1.4. No oral or written information or advice given by PTI, its dealers, distributors, agents or employees shall create a warranty or in any way increase the scope of any warranty provided herein.
- 6.2.1.5. The limited warranty does not apply to software provided to you free of charge, for example, updates, pre-releases, demonstration, product sampler, or software that has been altered by you or your representative, to the extent that such alteration caused a defect.
- 6.2.1.6. This Limited Warranty is void if failure of the software has resulted from force majeure, accident, abuse, or misapplication. Any replacement software will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

7. Limitation of Liability

- 7.1. To the maximum extent permitted by applicable law, in no circumstances and under no legal theory, tort, contract, or otherwise will PTI Integrated Systems (PTI), our officers and employees (past, current and future), our suppliers or dealers be responsible for any indirect, special, incidental, punitive, cover or consequential damages including computer failure or malfunction, lost profits, lost savings, lost business, business interruption, loss of data, penalties, fines or other either incidental or consequential damages by any party, without limitation, arising out of the use of or inability to use the software, or based on the configuration or failure to perform of the software or based on any data entry by or information provided by a PTI employee with regard to the software. PTI's cumulative liability under this EULA shall be limited to and never exceed the amount of license fees paid to purchase the software giving rise to such liability or fifty United States dollars (\$50), whichever is greater.
- 7.2. PTI, our suppliers, and our dealers shall have no responsibility or liability if the software has been altered in any way, or for any failure that arises out of use of the software with a hardware configuration, platform, or operating system other than that recommended by PTI.
- 7.3. The foregoing limitations on liability are intended to apply to all aspects of this EULA.
- 7.4. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this limitation and exclusion may not apply to you.

8. Hold Harmless

- 8.1. You agree to indemnify, hold harmless and defend PTI, our officers and employees, agents, and dealers at your expense against any claims or demands, actions, proceedings and suits and all related liabilities, losses, actions, damages, penalties, fines, settlements, or claims (including all reasonable expenses, costs, and attorneys fees) without limitation arising out of or relating to any use of, or reliance on, any PTI software or equipment

9. Governing Law Jurisdiction

- 9.1. This EULA shall be governed by and construed under Arizona law as such law applies, except as governed by Federal Law. You hereby consent to the exclusive jurisdiction and venue of the state and federal courts sitting in Maricopa County, Arizona. To resolve any disputes arising under this EULA. In each case, this EULA shall be construed and enforced without regard to the United Nations Convention on the International Sale of Goods. Some states do not permit disclaimers of certain warranties or limitations on certain types of liability under certain circumstances; consequently some of the foregoing disclaimers and limitations may not be applicable to you, in whole or in part.
- 9.2. In the event of any conflicts between foreign law, rules and regulations, and the Arizona's law, rules, and regulations, then the Arizona law, rules, and regulations shall prevail and govern.
- 9.3. The limitations or exclusions of warranties, remedies or liability contained in this EULA shall apply to you only to the extent such limitations or exclusions are permitted under the laws of the jurisdiction where you are located.
- 9.4. Any arbitration, lawsuit, or other legal challenge to this EULA shall be pursued only in Maricopa County, Arizona, USA.

10. Enforceability

- 10.1. If any part of this EULA is found by a court of competent jurisdiction to be invalid, unlawful or unenforceable to any extent, that provision shall be reformed only to the extent necessary to make it enforceable and will be enforced to the maximum extent permissible, and the remaining terms, conditions and provision will continue to be valid and enforceable to the fullest extent permitted by law.

11. User Remedies

- 11.1. PTI's and its suppliers' entire liability and your exclusive remedy shall be, at PTI's option, either refund of the purchase price or the repair or replacement of the software. Outside the United States, neither these remedies nor any product support services offered by PTI are available without proof of purchase from a PTI authorized distributor.
- 11.2. Any legal challenge to this EULA must, at the sole option of PTI, be pursued via arbitration in Maricopa County, Arizona, USA. You agree to select an Arbitrator that is a member of a major national arbitration association that is acceptable to PTI and you agree to pay for any and all arbitration fees. You also agree that the arbitration will be binding and that you will pursue no further legal challenges, lawsuits, or appeals before or after the arbitration.

12. Upgrades and Updates

- 12.1. PTI may from time to time present programming fixes, updates and upgrades (collectively "updates") to you, including version updates to the software. You may accept or reject such updates to you, including version updates at your sole discretion as long as you acknowledge that any obligation PTI may have to support the previous versions of the Software are ended upon availability of the update.
- 12.2. If the Software is an update to a previous version of the software, you must possess a valid license to such previous version in order to use such update. All updates are provided to you on a license exchange basis. You agree that by using an update you voluntarily terminate your right to use any previous version of the software. As an exception, you may continue to use previous versions of the software on your computer after you use the update but only to assist you in the transition to the update, provided that the update and the previous versions are installed on the same computer; the previous versions or copies thereof are not transferred to another party or computer unless all copies of the update are also transferred to such party or computer.
- 12.3. Notwithstanding any other terms in this EULA, if the software is licensed as an upgrade or update, then you may only use the software to replace previously validly licensed versions of the same software. You agree that the upgrade or update does not constitute the granting of a second license to the software (i.e., you may not use the upgrade or update in addition to the software it is replacing, nor may you transfer the software which is being replaced to a third party).
- 12.4. Unless explicitly stated otherwise, any new features that augment or enhance the current Software, including the release of new properties, shall be subject to terms of this Licence.

13. Agreement

- 13.1. Complete Agreement
 - 13.1.1. This EULA constitutes the entire agreement between the parties with respect to the use of the software and the related documentation, and supersedes all prior or contemporaneous understandings or agreements, written or oral, regarding such subject matter. No amendment to or modification of this License will be binding unless in writing and signed by the Chief Executive Officer of PTI.
 - 13.1.2. Installation or use of this software for any period of time constitutes your acceptance of this EULA and agreement to be subject to its contents.
 - 13.1.3. You agree that any varying or additional terms contained in any purchase order or other written notification or document issued by you in relation to the Software licensed hereunder shall be of no effect.
 - 13.1.4. The failure or delay of PTI to exercise any of its rights under this EULA or upon any breach of this EULA shall not be deemed a waiver of those rights or of the breach.

13.2. Termination or EULA

- 13.2.1. This License is effective until terminated. You may terminate this License at any time by destroying the Software and related documentation and all copies thereof. This License will terminate thirty (30) days after receipt of the software, unless the software is registered with PTI with appropriate compensation and registration information.
- 13.2.2. In the event that you fail to comply with this EULA, PTI may terminate the license and you must destroy all copies of the software (with all other rights of both parties and all other provisions
- 13.2.3. This EULA is immediately terminated in the event you are refunded the purchase price for whatever reason and you may no longer use the software without the written consent of PTI.
- 13.2.4. Upon termination of this license you must destroy the software along with any backups and copies, uninstall it from any computers, and you must no longer use the software in any way.
- 13.2.5. It is your responsibility to comply with the terms of this EULA and to obey the laws of your jurisdiction. Your rights under this EULA will terminate immediately and without prior notice if you violate any term of this License, including violating any applicable laws or rights of any third party including the intellectual property rights of any such third party. You may be subject to legal action if you continue to use the software in violation of this EULA.
- 13.2.6. Termination of the EULA by either party cancels any rights that you have under this EULA but does not terminate any of PTI's rights or protection under this EULA. All provisions which must survive in order to give effect to their meaning, shall survive any expiration or termination of this EULA, including without limitation all of your representations, responsibilities, and indemnification obligations.

14. Technical Support Services

- 14.1. PTI may provide you with Technical Support services related to the software. With respect to technical information you provide to PTI as part of the Technical Support Services, PTI may use such information for its business purposes, including for product support and development. PTI will not utilize such technical information in a form that personally identifies you.
- 14.2. PTI Technical Support service may have fees and costs associated with using or being licensed to use the software over and above the original purchase price of the software. By using or installing the software, you agree to pay these fees and costs, including any reasonable collection fees, late fees, and interest in a timely manner as a part of this EULA.

15. Contact Information

All questions concerning this EULA shall be directed to our Customer Service Manager at PTI Integrated Systems at 9160 East Bahia Drive, Scottsdale, Arizona 85260. (480) 991-1259.

Standard 2-Year Equipment Warranty

Preferred Technology, Inc. dba PTI Integrated Systems (PTI) warrants PTI manufactured products to the original purchaser (User) to conform to its own specifications, and to be free from defects in materials and workmanship under normal use and service for period of 24 months from the date of shipment provided PTI recommended installation and maintenance procedures are followed by the User. Within the warranty period, PTI will repair or replace with new or remanufactured equipment, at its option, all or any part of the product(s) covered under warranty. Further, this warranty does not extend to equipment or component systems manufactured by others and sold by PTI. In such cases, the original manufacturer's warranty shall apply and the User is responsible for contacting the manufacturer for support. Replaced or repaired equipment, components or parts are warranted only for the remaining portion of the original warranty period or 90 days, whichever is greater. PTI will not be responsible for any User incurred costs or damages resulting from the dismantling and/or re-installation of covered equipment.

This warranty shall not extend to damages resulting from improper installation or maintenance, misuse, failure to follow installation and operating instructions, alteration, abuse, accidents, tampering or vandalism, connection to improper power sources, fire, flood, lightning, power surge or other acts of nature or force majeure. This warranty shall not extend to normal maintenance, which the User is expected to provide.

To exercise the warranty, the User must be given a Return Material Authorization (RMA) number by PTI. Before equipment is returned to PTI for repair, the User must contact PTI's technical support department for assistance with troubleshooting and verification that the product needs repair. RMA numbers will ONLY be provided after completion of reasonable troubleshooting by qualified PTI technical support personnel. The User, or service personnel hired by the User must make a reasonable and valid attempt to verify that the equipment actually needs repair by following the suggestions of PTI technical support department staff. Equipment deemed faulty and requiring warranty work shall be returned to PTI at the User's expense. All warranty repairs will be performed at PTI's headquarters in Scottsdale, Arizona. PTI will not service equipment at the User's site unless a separate, expressed service agreement is arranged in writing between PTI and the User. Equipment returned without prior technical support and RMA number will be considered outside of warranty coverage, and all standard repair charges and return shipping will apply.

This warranty is in lieu of and excludes all other warranties, obligations or liabilities, expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. In no event shall PTI be liable for any incidental or consequential damages due to any defect or failure of the equipment.

Contact PTI



PTI Integrated Systems World Headquarters

9160 East Bahia Drive
 Scottsdale, AZ U.S.A. 85260
 (800) 331-6224 or (480) 991-1259
 Fax: (480) 991-1395
 www.ptiaccess.com

Sales Email: sales@ptiaccess.com

Customer Service Email: service@ptiaccess.com

Technical Support Email: support@ptiaccess.com

Accounting and Billing Email: accounting@ptiaccess.com



PTI East

625A Pulaski Highway
 Joppa, MD U.S.A. 21085
 (800) 933-3716
 Fax: (410) 679-7688
 sales@ptieast.com



PTI Los Angeles Presentation Center

81 Columbia # 201
 Aliso Viejo, CA U.S.A. 92656
 (800) 331-6224
 sales@ptiaccess.com



PTI Europe

Unit 1C Twickenham Trading Estate
 Rugby Road
 Twickenham, Middlesex, TW1 1DG
 United Kingdom
 +44 (0) 20 8892 6317
 Fax +44 (0) 20 8744 9208
 sales@ptieurope.com
 helpdesk@ptieurope.com



PTI UK

Unit 10, Nelson Trading Park
 The Path, London SW19 3BL
 United Kingdom
 +44 (0) 208 540 2713
 Fax +44 (0) 208 543 7952
 www.ptisecurity.co.uk
 sales@ptisecurity.co.uk
 helpdesk@ptisecurity.co.uk



PTI Australasia

35 Prosperity Place
 Gebung, Queensland 4034
 Australia
 61 7 3216 5524
 Fax: 61 7 3865 1713
 sales@ptiaustralasia.com
 support@ptiaustralasia.com



PTI Asia

34 Joo Koon Road
 Jurong, Singapore 628986
 (65) 68629365
 Fax: (65) 68620970
 bp@steelstorage.com.sg

Glossary

Access Areas	Parts of the site where access is controlled by keypads or Wiegand devices. Access Areas can be inside other Access Areas. For example, most sites will have a Default Access Area that is the entire site inside the fence line. Within that access area may be several buildings, each with their own keypads for access. Inside each building may be several floors, each with their own keypads for access. Inside each floor may be several rooms, each with their own keypads for access. These would all be access areas.
Access Controlled	Preventing access to or egress from an enclosed area by using a fence or wall with a gate or door in it. Persons wanting to enter or exit the enclosed area must enter a code or present a card at a device controlling the door or gate.
Access Levels	Used to add groups of people with similar access privileges. For example, if a site has managers, employees, and customers with two different types of access, they can setup access levels to make it easier to add each of these types of users without having to remember all of the variables every time one is added. Access Levels are a combination of Access Areas and Time Schedules.
Activate Time	The amount of time in Hours, Minutes, Seconds, and tenths of a second that a relay will remain activated when triggered.
Activation	PTI's process of changing the software from Demonstration mode to live-use mode after the software has been paid for.
Active in Open State	This option is chosen when a relay has been wired backwards. It allows the relay to be used without rewiring by switching its functional state in the software.
Address	The site's street number name when entering site setup information. Also, another name for AI Device ID in connection with previous Falcon Systems.
Administrator	User with full rights to setup or change any part of StorLogix.
Adobe Reader	Program used to open and read .pdf documents.
Advanced Options	Options in the Setup Screens that offer a higher level of customization for complex site setups.
AI Device	Any Keypad, Multiplexer, Relay Board, or Wiegand device. In previous Falcon Systems, this was referred to as a Remote.
AI Device ID	The unique identifier number programmed in to each AI Device to differentiate it from other AI Devices when communicating to the Falcon XT. Referred to as Address in previous Falcon Systems.
AI Device to Camera	To associate an AI Device to a specific camera to allow any events from that device to show the video from that camera at that time when the event is clicked on.
AI Devices Baud Rate	Communications speed between the AI Devices and the Falcon XT. This is programmed at each AI Device AND in StorLogix and must match between all of them.
Alarm File or alarm.alm	This is the file that associates the unit number painted on the door (unit name) with the multiplexer address (Device ID) and channel or input number.

Alarm Shunt	A relay that bypasses an alarm switch device for a specific period of time. For example, the front door alarm may be shunted for 60 seconds to allow the employee to exit the site after setting the alarm without triggering the alarm. After 60 seconds, then the door alarm would be live.
Alarm Zone	These allow a site with multiple sirens to create areas or zones where the sirens sound only for alarms that occur in that area.
Alerts	Emails that StorLogix can send based on events. See Chapter 10.
Allow Exit with Door Open	If a unit door has an alarm switch on it, this setting can be turned on to remind the user that the door to their unit was not closed.
Allow Manual Trigger	An option to allow a gate or door to be opened by pressing F6 on the keyboard at the StorLogix computer.
Anti-passback	Anti-passback is used to prevent 'tailgating' where a user follows someone else onto the site or into an area without using their own code. It also helps prevent users from 'passing back' their card to another user who forgot their card. The ultimate goal is to keep track of who is actually on-site and prevent access to unauthorized persons. Anti-passback functions are meant for higher security locations where employees and users can be well trained to use their access cards correctly and not tailgate. High security sites with guard booths and/or an active security team will find this to be a very helpful function. Sites with high user turn-over like many self storage have with their customers will find this function to be frustrating as customers will often tailgate onto the site or off and get stuck when they try to come back.
Anti-Virus	Software that helps protect the computer from viruses.
Area in Lockdown	All access is blocked. No one can enter or exit the affected area at all.
Area Suspended	No one can enter the area affected, but anyone with valid access is allowed to exit the area if they are already inside it.
Automatic Login	This function enables a user to double-click on the StorLogix icon and automatically open StorLogix without entering a password.
Auxiliary Siren	A siren connection on multiplexers that will sound the siren if any alarm occurs on the site.
Bad Attempts Limit	This is used to help prevent code-hacking. If someone tries to guess codes by entering code after code, this can keep them from succeeding. A recommended setting for this is 3 - 5 attempts. That gives legitimate users the ability to make a mistake or two without getting locked out while interfering with someone attempting to guess codes. For example, if this is set to 3 attempts. After a potential thief enters three incorrect codes in a row, then on the fourth attempt, the keypad will prevent access (even for correct codes) for 60 seconds. Any key that the thief presses during that time will reset the 60 seconds. After the 60 seconds is up, the keypad returns to its normal state allowing new codes to be entered. Setting this to 0 turns off the function.
Baud Rate	Communications speed between devices. See AI Device Baud Rate and Host Computer Baud Rate.

C:\	The C drive on a computer. Usually this is the hard drive of the computer where programs and other information is stored, but occasionally, the computer is setup with a different letter of the alphabet designating the hard drive.
Card Only	For keypads with card readers, it lets the keypad accept access using just a card.
Card+Pin	For Apex keypads with card readers, this high security feature requires a card and a pin number to prevent stolen cards from gaining access.
CD	Compact Disc. Device used to store data and programs for computers.
Change DB	Change database allows the database to be changed for multi-site setups.
Channel	An individual alarm input point on a multiplexer, APEX keypad, 8-channel relay board, or Falcon XT.
Check In/Out	This function allows a keypad to be setup so that everyone must check-in at this location (such as in the office) before they can use any other keypad or open any alarmed door on the site. They must also check out at this keypad. Often this is used when the site is accessed through one main lobby with multiple wings and hallways that are access controlled beyond the lobby. A user must checkin at the lobby keypad before they can use any other keypad or alarmed door on the site.
Code Only	For keypads that do not have cards, this lets the keypad function by using the touchpad.
Comm Count	This is the number of communication errors that the Falcon XT will ignore before reporting a Communications Off event. This can be turned down during troubleshooting for communications errors, but generally this should be set at 10. It is not a good idea to turn this number up any higher.
Comm Off-Line	This is when an AI Device no longer is communicating with the Falcon XT.
Communication Alarms	Alarm events in StorLogix that may sound the siren if an AI Device stops communicating due to vandalism, poor installation, etc.
Communication Port	A connection point on a computer that allows other devices to be connected to the computer including the Falcon XT.
Contrast Code	This is only used when the Falcon XT is connected to previous PTI keypad models manufactured before 2000, that did not have a backlit display, so the contrast had to be adjusted for lighting conditions. This contrast code could be entered on the keypad allowing the operator to press * to darken the screen or # to lighten. If the keypads are manufactured after the year 2000, this is not an issue as the displays are backlit. The Contrast Code can NEVER be used as an access code.
Counted Late Exit	Exit is allowed after time schedule hours, but the user is limited to the number of time that they can use this feature. Each time they exit after time schedule hours, it is counted and when it reaches the number set in the Late Exit Count Limit, they are suspended and must be reactivated by an administrator.

D:\	The D drive on a computer. Usually this is the CD or DVD drive, but occasionally, the computer is setup with a different letter of the alphabet designating the CD or DVD drive.
Data Format	For wiegand devices this is the specific protocol type for the device. There are many types of these. The PTI system is compatible with 26 bit, 30 bit, 31 bit, and 34 bit. Refer to the wiegand device manufacturer's instructions for the specific Data Format for the device.
Database	A collection of information organized in such a way that the computer program can quickly access it.
Delay before Sounding	Advanced Alarm Zone setting that allows a delay before the alarm sounds. This can be used to allow entrance to a property and give the user time to go clear the alarm before it sounds.
Demonstration Mode	Feature of StorLogix that allows the program to be run for 30 days prior to purchase to allow the client time to become familiar with the product and test the functions.
Desktop	The main screen of Microsoft Windows where the icons and start bar are found.
Device Tamper	Tamper switches built into AI Devices. These always report as an alarm even if authorized users are logged into the area.
Door Alarm Contact	Hard wired switches that are installed on doors to indicate if the door is open or closed.
Door Controller	A wiegand device or keypad that controls the access to a door.
Door Forced Open	Doors that are directly controlled by keypads or wiegand devices for access can have door contact switches placed on them to activate alarms if the door is forced open without entering a valid code or card.
Door Held Open	Doors that are directly controlled by keypads or wiegand devices for access can have door contact switches placed on them to activate alarms if the door is held open longer than a preset amount of time.
Door Held Timeout	This is the length of time that an access controlled door with a door contact switch can be held open before the Door Held Open alarm is activated. See Door Held Open.
Door Input	An alarm input point for door contacts
Door Switch	Another name for Door Alarm Contacts.
DVR	Digital Video Recorder.
DVR Integration	Allows a compatible DVR to be connected with StorLogix so that events can be associated with cameras making video quick and easy to locate.
DVR IP Address	A unique identifier number assigned to Digital Video Recorder computers on a network to differentiate them from each other computers or DVR's.
Easy Link	Program used to interface StorLogix to various Management Software programs.
Elevator Control	Using Relay Boards, StorLogix can be programmed to prevent users from getting to floors in a building that they should not have access to. When the user enters their code at an elevator keypad, only the button to the floor with their unit will light.

Elevators	For the purposes of StorLogix, this refers only to elevators controlled by relays to limit elevator access to authorized personnel.
Entire Alarm System On	This is a function in the Falcon XT setup that allows the entire alarm system to be turned off by deselecting this check box. Generally, this would only be done for maintenance or troubleshooting purposes.
Entry/Exit	This is used primarily when there is only one keypad on a site with alarms. Users must come and enter their code at this keypad to turn off the alarm at their unit. The second time they enter their code at this device, it turns the alarm back on.
Ethernet	A type of Network setup for computers to allow multiple computers to be connected together.
EULA	End User License Agreement. The list of rights and responsibilities of a software purchaser in agreement with the software seller.
Event	Occurrences and actions within StorLogix that are recorded and may appear on the event log. For example, when a user presents their card for valid access at a gate, at least four events will occur: "Known Card Presented", "Access Granted", "Relay Activated", and "Relay Deactivated". Each of these 'events' will appear as a line item on the Event Log (if selected to show within Events to View).
Event Sounds	Sounds in StorLogix that can be heard if the computer has speakers. These can alert the user to different events. StorLogix has several default sounds, however, the user can change these if desired. For example, a siren sound will occur when an alarm event happens.
Events to View	A setup wizard in the setup screen that allows events to be shown or not shown on the event log. Not showing them does not delete the event; the event still is there and can be reviewed later if necessary. This wizard also allows sounds and alerts to be associated with each event.
Export	To send data from one program to another. For example, to save a copy of the alarm file created in StorLogix to another location.
Facility Code (Prox Cards)	This is an extension of the Proximity Card code length in most types of proximity cards. Generally, this will be left on. In some cases, when converting an older proximity card system to the StorLogix, the site may not be using the facility code and will need to turn this off.
Falcon XT	Controller for AI Devices programmed and operated using StorLogix.
Fence line	The enclosure for access control. May be a wall or fence. Anything that forces entry to a site through a controlled door or gate.
Floor 1	The lowest floor on a site. This is not always the ground floor. Sites with sublevels or basements that the elevator accesses will have Floor 1 as the lowest subfloor serviced by the elevator.

Free Late Exit	This is the option that most sites will use. Customers can freely enter and exit the site within their authorizations during their time schedule. After their time schedule is closed, they can still freely exit the site, but the exit will report in the event log as a late exit to allow tracking of this behavior.
From Access Area	The area outside an access controlled "To Access Area". For example, in most sites, the primary From Access Area will be called Offsite (everything outside the fence line). The primary To Access Area would be called On-site (everything inside the fence line). Other access controlled areas inside the site might be further To Access Areas. For example, an access controlled building inside the site would have a From Access Area of On-site and a To Access Area of Building A. Building A may have an access controlled Wine Storage inside it with a From Access Area of Building A to a To Access Area named Wine Storage. See From Access Area.
Glass Break Sensor	Sensors that can detect if a window is broken by monitoring for the sound frequency of the glass breaking. Refer to Manufacturers Instructions for installation and operation of these devices. In StorLogix, these always report an alarm, even if authorized users are logged into the area.
Highest Floor Number	The highest floor that an individual elevator actually services. This becomes very important in high rise buildings where some elevators only service certain floors.
Holiday	A program setting in StorLogix that allows the regular access hours to change or be locked out on certain days of the year.
Holiday End Time	The actual time during the day on a holiday date when the Holiday hours end. This allows regular access to resume after this time.
Holiday Start Time	The actual time during the day on a holiday date when the Holiday hours begin. Regular access hours are active until this time.
Host Computer Baud Rate	The communications speed between the StorLogix computer and the Falcon XT. This baud rate is set in StorLogix and must match in the Windows Device Manager.
Icon	A small picture that represents a program. Generally, clicking on the icon with the mouse will open the program represented.
Import	To use data created by another application. For example, to use an alarm file created in Falcon 2000 or word pad to input the unit information into StorLogix.
Input	A point in the system that alarm switches, motion sensors, glass break sensors, door contacts, or tamper switches can be connected.
Input Tamper	A tamper switch installed on devices other than AI Devices by an installer. These may include tampers on motion sensors, junction boxes, security cabinets, etc. In StorLogix, these always report as an alarm even if authorized users are logged into the area.
Input to Camera	To associate an input to a specific camera to allow any events from that input to show the video from that camera at that time when the event is clicked on.

Inputs to Units	Inputs to Units are alarm switches that are associated with specific units. This may be door switches on the unit door, motion sensors inside the room, or photobeams across an RV space.
Install	To load the software onto the computer.
Installation Folder	The folder on the computer where the files are kept that are required to run a program.
Invalid Access Attempt	When someone enters a code or presents a card at a keypad or wiegand device that is not allowed access do to an incorrect code entry, being outside of their time schedule, trying to enter an access area that they are not authorized for, or trying to enter when they are suspended. The keypad or wiegand device will deny access. See also Valid Access Attempt.
IP Address	A unique identifier number assigned to computers on a network to differentiate them from each other.
Late Exit	Exit after the time schedule assigned to the user.
Lighting Area	Lighting areas are relays connected to lights in hallways, stairwells, building exteriors, or units that are set to come on for certain users entering that access area.
Load	Another name for installing software.
Local Computer	The computer that is being used or worked on at the moment.
Log Off Time of Day	Optional setting that clears all users off the site at a certain time every day to remove users that may have tailgated off the site from the access. This should not be used on-sites with 24 hour access.
Logical Anti-Passback	This helps to control access with anti-passback. If this is set, a user cannot gain access to an area if they aren't already in the area before it. For example. If a site has an access controlled building on it as well as access control at the gate, a user can not use the keypad to access the building unless they first used the keypad to access the gate. This works off of the TO and FROM areas that are setup for each access device in the Setup AI Device Properties Function previously in this chapter.
Login	To enter a valid user name and password so that StorLogix recognizes the user and allows them access.
LogixServer	The program that controls communication between the StorLogix Software and Falcon XT
Logon ID	ID used with password to gain access to the software. Usually the person's name.
Lowest Floor Number	The lowest floor that an individual elevator actually services. This becomes very important in high rise buildings where some elevators only service certain floors.
Management Software	Software program used to manage a site. In self storage, these programs are used to rent units, send letters, assess fees, sell merchandise, and track the collections and auction process.
Maximum AI Devices	Set this to the same number as the highest AI Device ID (address). It is the highest AI Device ID that the Falcon XT will look for while polling AI Devices.

Maximum AI Devices	Set this to the same number as the highest AI Device ID (address). It is the highest AI Device ID that the Falcon XT will look for while polling AI Devices.
Maximum Code Size	This is used when the site uses magnetic swipe or proximity cards for access control. The Falcon XT automatically converts the code on the card to a 10 digit number for access. Some management software programs have a code length limit. If the Falcon XT is interfaced to one of these programs, the code size can be turned down to the required length for that software. Check with the management software manufacturer for their limitations. This is not an issue with TaskMaster as codes can be any length up to 10 digits.
Maximum Users in Area	The number of users that are allowed inside an access area at any one time based on a count of the number of users entering the area minus the users that have left the area. Anyone trying to enter the area once the maximum number is reached will be denied access.
Menu Bar	The bar immediately below the Window bar that allows access to drop down menus that contain most of the StorLogix functions by clicking on a word.
Motion Sensor	A device that monitors for motion in an area, usually by sensing infrared heat traveling across an area. In StorLogix, these only report as an alarm if there is no authorized user logged into the area. If there is an authorized user logged into the area, no alarm is reported.
MSDE	Microsoft SQL Server Desktop Engine is the database engine used by StorLogix.
Multiplexer OR Mux	An AI Device used to combine multiple input signals into one output data signal. It is a connection point for door alarms that feeds the information from multiple doors back to the Falcon XT.
Mux ID	The AI Device ID for a Multiplexer programmed using the switches on the multiplexer circuit board.
Network	Two or more computers linked together to access shared files and programs.
No Late Exit	Exit is limited only to Time Schedule hours. If the user's time schedule allows access from 8:00 am to 5:00 pm, they CANNOT exit the site after 5:00 pm. This is only for High Security Facilities and should NOT be used on most sites.
Nova	One of the two Credit Card Processing companies that can be used with PayXpress. See Also Paymentech.
Off Time	The time in seconds and tenths of seconds that a relay is off between repeats. See Repeat Counts.
Off-Site	For the purposes of StorLogix, this is the area outside of the fence line, that is the area that is not inside an access area. Essentially, it is the rest of the world other than the site.
On Time	The length of time that an alarm siren will sound during day or night hours.
On Time – Day OR On Time – Night	The length of time that a lighting zone or alarm zone siren will stay on for if activated during Daytime or Nighttime hours.
On-Site	The area within the fence line of a site that is access controlled. For StorLogix purposes, this is anything inside the main Access Area.

Operator	A User that has access to the StorLogix software. Generally an employee of the site.
Output	Another name for a relay in StorLogix.
Panic Alarm	An alarm button that is setup to automatically trigger an alarm zone when pressed. This may be on a pendant worn by the site manager or placed under a desktop. This can trigger a silent or audible alarm.
Pass Through Lighting Area	A lighting area that a user must go through to get to their unit that is inside a different lighting area.
Passback Setting	This setting in the Setup AI Device Properties wizard allows each keypad or wiegand access device to be setup with specific properties of the Anti-passback settings or to be exempt from the site Anti-passback rules. See Anti-passback for more information.
Password	A unique private identifier from 1 to 15 characters that is used along with the Logon ID for an Operator to gain access to the StorLogix software.
Paymentech	One of the two Credit Card Processing companies that can be used with PayXpress. See Also Nova.
PayXpress	Module in TaskMaster and StorLogix that allows credit card payments to be made from an APEX keypad so customers can pay at the gate.
pcAnywhere	A software program by Symantec that allows one computer to 'dial in' to another computer and control it. Generally used for technical support and for home office control of remote sites.
PDF file (.pdf)	Document type created by Adobe Acrobat that allows documents to be shared and read without being changed.
Physical Relay	An actual tangible electronic relay switch. For Example: there are two relay switches located in an APEX keypad that can be used to open gates or doors. See Also Relay and Virtual Relay.
Poll Timeout	The Falcon XT constantly polls the AI Devices to see if they have any information (such as requests for entry). This occurs many times each second. The Poll Timeout is the amount of time that the Falcon XT will wait for an answer from the device before recognizing that there is a communication error and moving on to poll the next device. This number should be set between 10 - 30 on most systems. On systems using Wireless RS485, the Poll Timeout should be set higher to 150 - 200.
Power Fail	This is an alarm event that occurs when the Falcon XT device loses power and is running off of its battery power.
Preferences	System-wide user settings that can be customized for the site.
Quick Help Bar	Bar on the left side of the task bar that contains help text giving some explanation of the icon that the cursor is floating over.

Rearm Time	In connection with Units, this serves two functions: 1) It is the time from the moment that the user closes their unit door until the unit alarm is rearmed to protect the unit. 2) It also serves as the amount of time that the user has from the moment that they log onto the site to open the unit door. If they do not open the unit door before the timer runs out, then the alarm will sound when they open the door. Rearm time must be set high enough to allow the user to get to their unit, including time for them to do things such as unload the car, get a cart, go to the office, and pay their bill, etc. Generally, it is a good idea to figure out the amount of time it takes to walk from the parking lot space farthest from the building to the unit that is farthest away from the parking lot. Be sure to add some additional time for any other things the user might do on the way.
Rearm Wait Time	The amount of time after an area has been entered before users in the area are cleared and the alarm is reset. This is an optional advanced function of Access Areas and is generally used for stairwells or other areas that users must pass through and should not remain in.
Red Letter Fields	These are required fields in StorLogix.
Region	An optional field in StorLogix to identify the site when a single company owns multiple sites. (i.e. Southwest, Pacific, Asian, etc).
Register	During the licensing and activation process, this lets PTI know the purchaser of the software.
Relay	A switch located in electronics used to control another device. May be physical or virtual. See Also Physical Relay and Virtual Relay.
Relay Board	An AI Device that has multiple relays on it. Generally these are used to control elevators or lighting zones, but may also be used as additional relays on a site.
Relay to Camera	To associate a relay to a specific camera to allow any events from that relay to show the video from that camera at that time when the event is clicked on.
Remote Assistance	Windows XP function that allows one computer to 'dial in' to another computer and control it. Generally used for technical support and for home office control of remote sites.
Repeat Count	The number of times that a relay will trigger after being activated. These are offset by the off time.
Request to Exit Inputs	These are inputs in the system that are used for exit on Access Controlled Doors so that there doesn't have to be a keypad on both sides of the door. A push button is generally wired into an input in the keypad or the Falcon XT and it is then designated as a request to exit input for that door in StorLogix. When a user pushes that button, it will trigger the relay allowing the user to exit the door without setting off the Door Forced Open alarm.
Required Level On-Site	An optional function of Access Levels that can require someone of a higher level be on-site before a person of a lower level is allowed access. For example, the system could require that a manager be logged into an office area before an employee could gain access or an employee must be logged on-site before a customer can gain access to the front door.

Run Command	A command on the Start bar that allows programs to be run directly by typing in the correct destination folder and program name without using an icon.
Security Level	These are the various preset levels of access permissions and privileges for the computer operators, including which functions in StorLogix they have access to.
Serial Port	A 9-pin communications port. One of the three ways that the Falcon XT can be connected to the StorLogix computer.
Setup Screen	The screen in StorLogix where almost all of the setup for StorLogix and Falcon XT occurs.
Setup Units	Function in StorLogix to enter the units for the site.
Silence Alarms	A function in StorLogix to turn off all alarms that have been activated. Using a virtual relay, this can be setup with an alarm input button to allow a site employee to turn off the alarms remotely by pushing a remote button or pendant button.
Site Code	An optional four digit identifier that can be used to identify individual sites when a company owns multiple sites. Many companies have store numbers that this could be used for.
Start Bar	The bar that is usually along the bottom of a Windows Desktop showing what programs are open.
Start Button	The button usually at the bottom left corner of a Windows Desktop on the Start Bar that access many of the programs and functions on the computer.
Start Time – Day	This is the beginning of daytime hours for a site for use with alarm zones and lighting areas. This allows the site to set their daytime hours to whatever they need to meet individual site needs or local code restrictions on alarm sirens.
Start Time – Night	This is the beginning of nighttime hours for a site for use with alarm zones and lighting areas. This allows the site to set their nighttime hours to whatever they need to meet individual site needs or local code restrictions on alarm sirens.
Stop Rearm Time with Door Open	This allows the rearm time to stop counting down while a user has their door open and reset the timer to the full rearm time when they shut the door. Generally, this function should be checked. If it is unchecked, then the timer would continue counting down even while they are in their unit. This would only be unchecked if the site wants to limit the amount of time a user can be in a unit.
SVGA	Super Video Graphics Array. A graphics monitor display standard.
Swinger Shutdown	Roll-up doors sometimes shake with traffic vibration or wind due to poor installation, settling of the building over time, or broken tracks. If this becomes excessive, causing the door alarm to sound, then this function can be used to allow the system to ignore door state changes that do not last for a longer period of time.
Tamper Switch	An alarm switch that is triggered when a device is opened.
Task Area	The central part of the StorLogix screen where the Icons are found.
TCP/IP	A protocol for computer networks.

TCP/IP	A protocol for computer networks.
Time Schedule	Preset timetables used for access permission and scheduled functions in StorLogix.
Time Slots	Individual spans of time within a time schedule.
Time Zone	In StorLogix, this refers to the 24 zones of the earth used for setting clocks. In previous Falcon systems, this referred to a function that was similar to a combination of Time Schedules and Access Areas.
Timed - Counted Late Exit	This combines the features of Timed and Counted Late Exit, giving the user a grace period and only counting the late exit toward suspension if it is outside the grace period.
Timed - Logical Anti-passback	This option combines Timed Anti-passback and Logical Anti-passback, so a user cannot enter an area if they were not already in the logical area outside the one they want to enter and they cannot re-enter that area again within the timed setting unless they first exit it. See Timed Anti-Passback and Logical Anti-passback.
Timed Anti-Passback	This is usually used in a mangate or turnstyle situation to prevent a user from handing their card back to another person to use. It is a set amount of time during which a user cannot enter the same area without actually exiting the area first. Set the time limit in the Anti-passback Time (minutes field below).
Timed Late Exit	This option gives the user a Grace Period set in the field immediately below the Late Exit Mode. Exit from the site is allowed during time schedule hours for the user. After the time schedule is closed, then the exit is allowed during a grace period, but will record a Late Exit event in the event log.
Timed Operating Mode	Mode (code only, card only, or card+pin) that a keypad will operate with during a specific time schedule. Outside of that time schedule, it will operate in its assigned Operating Mode. Both Operating Mode and Timed Operating Mode are found in the Setup AI Device Properties wizard.
To Access Area	The area inside an access controlled fence line, building, or room. As you enter a code at a keypad or card at a reader, you cross from the "From Access Area" into the "To Access Area". For example, in most sites, the primary From Access Area will be called Offsite (everything outside the fence line). The primary To Access Area would be called On-site (everything inside the fence line). Other access controlled areas inside the site might be further To Access Areas. For example, an access controlled building inside the site would have a From Access Area of On-site and a To Access Area of Building A. Building A may have an access controlled Wine Storage inside it with a From Access Area of Building A to a To Access Area named Wine Storage. See From Access Area.
Tool Bar	The bar immediately beneath the menu bar that contains the five main functions of StorLogix.
Trip on Input	An advanced setting for lighting zones that allows them to be connected to motion sensors or other types of sensor to turn the light based on an input.

Turn OFF to Activate	This option is chosen when an input is installed backwards or the wrong type has been purchased. It allows the input to be used without rewiring by switching its functional state in the software.
Undefined Check-In Reporting	An optional setting in the Falcon XT setup that allows the system to display or ignore check-in events for devices that are undefined in the system.
Undefined Input Reporting	An optional setting in the Falcon XT setup that allows the system to display or ignore events for inputs that are undefined in the system.
Undefined Tamper Reporting	An optional setting in the Falcon XT setup that allows the system to display or ignore events for tamper switches that are undefined in the system.
Unit	Units are storage spaces, lockers, parking spaces, offices, rooms, suites, mailboxes, and other areas that are generally rented to clients. However, they can include manager units, apartments, storage sheds, dumpster areas, security closets, and any other enclosed area that might be monitored.
Unit Description	A 50 character field that allows more information about the unit for site reference purposes.
Unit in Area?	An optional limitation to Access Levels to allow a user access to any area in which they have a unit, but not to any area where they do not have units. Generally used with elevators or with multiple access controlled buildings on a site so that customers with units in multiple buildings or on multiple floors can access all of their units with one entrance code.
Unit Name	Generally, this is the number that is painted on the door of the unit or otherwise associated with the unit to uniquely identify it. In most cases the unit name will be a number (such as 100) or a number preceded by a building or floor identifier (such as A100 or 2-100). Other identifiers and words can be used base on use or location (such as RV-100, Box 100, Pine 100, or 1stAve 100). This field is limited to 10 characters and MUST match the unit name in site graphics.
Unknown Battery Change Reporting	An optional setting in the Falcon XT setup that allows the system to display or ignore device battery change events for devices that are undefined in the system.
Updates	A new version of software that contains improvements, new features, fixes, and other relevant changes.
UPS	Uninterruptible Power Supply – A device that provides high level surge protection, battery backup, and power conditioning for electronics devices.
USB	Universal Serial Bus. A communications protocol. One of the three ways that the Falcon XT can be connected to the StorLogix computer.
Use Facility Code	See Facility Code.
User	Any person that has access to the site, including customers, managers, employees, and others.
Vacant Alarms	An optional setting in the Falcon XT setup that allows the system to display or ignore alarm events from units that are not rented. This is a good feature to keep turned on to prevent vacant units from being used for criminal purposes.

Valid Access Attempt	When a valid user enters their code or presents their card at a keypad or wiegand device, the system will trigger the relay to open the door or gate. See also Invalid Access Attempt.
Version & Copyright Bar	The bar along the bottom of StorLogix that shows the current version and copyright information.
Virtual Relay	Switch commands setup in StorLogix that can perform actions within the system based on their status (either on or off). There is no actual physical switch involved, only system status. Generally these are used with Alarm Zones or LogixScript.
Virus	A malicious software program that is designed to damage a computer that is generally loaded on the computer without the operators knowledge and runs without permission.
WAV file (.wav)	.wav sound files are a type of sound file that can be used in connection with StorLogix events so that when the event occurs, the sound plays on the computer to get the operator's attention. This is setup in the Setup Events to View wizard in Chapter 9.
Wiegand Device	An AI Device that communicates with Wiegand Protocol Devices such as proximity card readers, fingerprint readers, or key fobs.
Window Bar	The Bar along the very top of the StorLogix screen that shows the Site Code and Site Name as well as having the maximize/ minimize and close icons.
Wizard	A utility that allows a program or process to be completed by going through a logical series of steps in order.

Index

Symbols

of Users in Access Area 188
.NET Framework 37, 40
.pdf 30, 45, 226, 234
.wav sound files 146, 147, 239
[D 154
[S 154
[T 154
[U 154
24 hour access 23, 63, 129, 136, 232

A

Access 217, 218
Access Areas iii, vii, viii, 10, 12, 13, 15, 16, 22, 23, 68, 89, 95, 97, 98, 99, 100, 101, 102, 103, 106, 111, 112, 116, 117, 120, 125, 135, 136, 137, 188, 189, 206, 208, 212, 226, 231, 232, 233, 235, 237
Access Levels iii, vii, viii, 9, 16, 22, 24, 97, 99, 102, 103, 106, 107, 206, 210, 226, 235, 238
Activate 10, 44, 73, 74, 75, 80, 81, 100, 125, 135, 164, 179, 180, 208, 226, 229, 238
Activation 27, 43, 44, 45, 226
Active in Open State 79, 80, 226
Activity 79, 179, 210, 212
Activity Log 179
Add a New Company 57, 59
Address 7, 10, 20, 22, 23, 44, 70, 80, 120, 131, 134, 136, 141, 147, 162, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 192, 193, 196, 208, 212, 218, 220, 226, 229, 232, 233
Administrator 7, 8, 17, 22, 50, 53, 59, 60, 61, 62, 67, 104, 105, 106, 226
Adobe Reader 27, 28, 30, 31, 32, 41, 45, 226
Advanced vii, 28, 55, 64, 67, 69, 72, 74, 75, 78, 79, 83, 86, 89, 95, 97, 100, 101, 106, 109, 114, 115, 116, 118, 123, 126, 127, 128, 131, 132, 133, 159, 163, 178, 226, 229, 235, 237
Advanced Options 55, 67, 78, 79, 86, 89, 127, 226
Agreement 217, 218, 222
AI Devices iii, 3, 10, 12, 19, 20, 22, 23, 24, 28, 64, 69, 70, 71, 72, 73, 75, 76, 77, 80, 81, 95, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 140, 142, 147, 159, 188, 192, 193, 195, 196, 197, 200, 206, 208, 210, 212, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 237, 239
AI Devices to Camera 20, 147
Alarm.alm 116, 118, 119, 120, 226
Alarm Contacts 76
Alarm File 109, 116, 118, 119, 120, 212, 226, 230, 231
Alarm Inputs 101, 124, 141, 200
Alarms & Events 60
Alarm Shunt 80, 227
Alarm Zones iii, 10, 11, 22, 75, 81, 83, 84, 85, 86, 95, 101, 127, 129, 188, 208, 227, 229, 239
Alerts iv, viii, 60, 85, 95, 146, 147, 149, 160, 162, 163, 189, 227
Anti-passback 100, 125, 126, 133, 134, 136, 137, 210, 227, 232, 234, 237
Anti-spyware 201
Anti-Virus 5, 22, 5, 22, 227, 201, 203, 227
Apex 6, 11, 84, 125, 129, 134, 154, 155, 157, 196, 228

Auction 219
 Audit 55, 62, 145, 220
 Automatic Login 55, 67, 227
 Auxiliary Sirens 10, 11, 22, 84, 129, 227

B

Backup 5, 25, 118, 218, 238
 Backup Data Files 5, 218
 Bad Attempts 126, 132, 134, 227
 Bad Attempts Limit 126, 134, 227
 Battery 19, 25, 212, 238
 Baud 19, 22, 23, 52, 67, 129, 208, 226, 227, 231
 Beep when Displayed 154, 156
 Buildings iii, 10, 12, 13, 14, 15, 22, 23, 71, 77, 81, 83, 85, 87, 88, 89, 90, 91, 92, 93, 95, 98, 101, 103, 106, 111, 120, 121, 126, 129, 133, 135, 136, 137, 142, 199, 206, 226, 229, 231, 232, 235, 236, 237, 238
 Business Hours , 12, 21, 63, 65, 74, 87, 88, 89, 93, 99, 100, 101, 102, 103, 126
 Business Name 220

C

Camera 6, 20, 22, 23, 24, 22, 20, 141, 142, 147, 226, 231, 235
 Camera Module 6, 220
 Card vi, 6, 10, 24, 125, 134, 135, 147, 151, 188, 228, 230, 233, 234
 Card+Pin 64, 125, 126, 134, 228
 Cards iv, viii, 6, 19, 60, 130, 135, 149, 150, 151, 152, 206, 210, 230
 CD 4, 27, 28, 45, 217, 118, 119, 28, 161, 217, 228, 229
 Change DB 53, 67, 228
 Channel 18, 20, 22, 76, 115, 120, 164, 198, 206, 226, 228
 Check In 125, 130, 134, 228
 Clear 59, 189, 206, 208, 210, 212
 Client Computer 167, 168, 173, 174, 175
 Code 219, 220
 Code-hacking 126, 134, 227
 Comm Count 131, 134, 210, 228
 Comm Off-Line 127, 134, 228
 Comm Ports 4
 Communication viii, 19, 22, 23, 38, 45, 52, 67, 127, 130, 131, 132, 134, 136, 162, 202, 208, 212, 221, 226, 227, 228, 232, 234
 Communications Errors 131, 132, 136, 234
 Company Info iii, 47, 50, 57, 58, 212
 Company Name 7, 33
 Computer 1, 2, 3, 4, 5, 8, 17, 19, 22, 23, 24, 25, 27, 28, 29, 30, 31, 34, 35, 36, 37, 38, 39, 40, 41, 42, 44, 45, 48, 51, 52, 53, 55, 68, 80, 107, 119, 120, 124, 146, 147, 160, 161, 48, 239, 48, 239, 51, 239, 166, 67, 174, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 179, 180, 193, 201, 202, 203, 214, 217, 218, 219, 220, 221, 222, 227, 228, 229, 230, 231, 232, 234, 235, 236, 237, 238, 162
 Configuration 5, 221
 Contact PTI iv, 2, 140, 200, 205, 225
 Contacts 23, 76, 101, 128, 135, 229, 231
 Contrast Code 131, 135, 206, 228
 Cookies 201
 Copyright ii, 54, 217, 218, 219, 220, 68, 239

Counted Late Exit 133, 135, 137, 228, 237
Counter 188, 210
Credit Cards 4, 6
Cross-reference iv, 196, 205
Custom Functions vi, 180
Custom Messages iv, vii, viii, 60, 127, 149, 153, 154, 155, 156, 157, 158, 159
Custom Messages Assigned to Devices 149, 159
Custom Messages Assigned to Users 149, 158

D

Data 218, 219, 221
Database 29, 45, 47, 48, 49, 51, 53, 59, 67, 146, 167, 168, 169, 170, 171, 172, 173, 174, 175, 180, 197, 203, 210, 212, 214, 228, 229, 233
Database Troubleshooter 197
Data Comm 200
Data File 178
Declarations iv, 205, 214, 215, 217
Decrement 189
Default 8, 9, 11, 15, 17, 31, 36, 39, 50, 53, 55, 56, 59, 63, 67, 84, 98, 102, 104, 127, 132, 230
Default Messages 153, 154
Delay Before Activating Relay 154, 156
Delay before Sounding 86, 95, 229
Demonstration 42, 176, 218, 221
Demonstration Mode 27, 42, 45, 229
Demonstration Period 43
Desktop 27, 28, 29, 40, 41, 45, 160, 229, 233, 236
Device Tamper 77, 80, 127, 135, 229
Digital Video vi, 6, 23, 41, 139, 140, 147, 166, 168, 229
Documents 217, 218, 221, 223
Do Not Show Again 55
Doors 3, 10, 13, 20, 22, 23, 24, 64, 73, 76, 77, 78, 72, 76, 77, 78, 79, 80, 81, 85, 89, 95, 101, 102, 106, 107, 109, 111, 114, 118, 127, 120, 121, 125, 127, 125, 127, 128, 129, 130, 132, 134, 135, 137, 141, 142, 153, 154, 156, 162, 164, 178, 189, 198, 199, 200, 214, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 238, 239
Door Contact 77
Door Forced Open 127, 135, 137, 229, 235
Door Held 127, 128, 135, 229
Door Switch 80, 229
Download 30, 33, 61, 201, 217, 221
Drive 4, 28, 45, 118, 120, 176, 193, 228, 229
Drivers 202
DVD 4
DVR iii, viii, 6, 23, 140, 141, 142, 147, 166, 141, 166, 23, 20, 140, 139, 168, 147, 166, 168, 170, 171, 172, 173, 174, 175, 203, 229

E

Easy Link 27, 28, 33, 34, 45, 33, 41, 33, 34, 33, 34, 35, 41, 45, 177, 229
Edit Current Company 57
Elevators iii, viii, 10, 12, 14, 20, 23, 24, 72, 81, 83, 88, 90, 92, 93, 94, 95, 98, 99, 103, 107, 125, 129, 132, 208, 229, 230, 231, 232, 235, 238
Email viii, 7, 44, 85, 146, 160, 162, 163, 225
End User License Agreement 35, 38, 45, 217, 230

Enroll AI Devices iii, 69, 70, 71, 72, 73, 76, 208
 Entry 221
 Entry/Exit 125, 135, 230
 Errors iv, 179, 218
 Error Log 179
 Ethernet 4, 23, 28, 52, 67, 4, 23, 28, 52, 67, 230, 202, 230
 EULA , 35, 223, iv, 230, 38, 45, 205, 217, 218, 219, 220, 221, 222, 223
 Event iii, vi, viii, 20, 22, 23, 24, 25, 41, 55, 60, 62, 67, 71, 77, 84, 85, 92, 93, 95, 98, 124,
 127, 130, 131, 133, 134, 135, 136, 137, 139, 140, 141, 142, 145, 146, 147, 160, 162,
 163, 164, 176, 179, 180, 193, 196, 212, 214, 220, 222, 223, 224, 226, 227, 228, 229,
 230, 231, 234, 235, 237, 238, 239
 Event File 179
 Event Filters viii
 Event Log vi, 20, 146, 147, 176, 230
 Event Sounds 55, 67, 230
 Events to View iii, 139, 145, 146, 147, 163, 230, 239
 EventViewer ii, 41
 Export 59, 109, 116, 118, 119, 120, 220, 212, 220, 230

F

F2000 folder 116, 176
 F6 74, 80, 227
 Facility 221
 Facility Code 19, 25, 130, 135, 230, 238
 Falcon 2000 116, 120, 178, 179, 205, 206, 208, 210, 212, 231
 Falcon 2000 to Falcon XT Function Cross-reference 205
 Falcon Base Unit 206, 208, 210, 212
 Falcon XT iii, vi, viii, 2, 3, 9, 10, 11, 14, 19, 22, 23, 24, 27, 28, 38, 41, 45, 68, 69, 70, 80, 84,
 123, 124, 127, 129, 52, 130, 53, 129, 25, 67, 130, 131, 132, 133, 134, 135, 136, 137,
 164, 167, 168, 169, 170, 171, 172, 174, 175, 176, 177, 191, 193, 197, 202, 203, 205,
 206, 208, 210, 212, 226, 228, 230, 231, 232, 233, 234, 235, 236, 238
 False Alarms 79
 Fees 219, 221, 222, 223
 Fence Line 15, 22, 98, 106, 120, 135, 137, 226, 230, 231, 233, 237
 Firewall 5, 167, 168, 169, 170, 171, 172, 173, 174, 175, 201, 203
 Flash Display 154, 156
 Floor vii, 13, 15, 23, 24, 88, 92, 93, 72, 93, 22, 93, 88, 93, 98, 99, 106, 111, 120, 121, 226,
 229, 230, 231, 232, 238
 Free Exit 128, 129
 Free Late Exit 133, 135, 231
 From Access Area 135, 137, 231, 237
 FROM and TO Access Areas 125
 FTP 221
 Full Site Reset 197, 200
 Functions 219

G

Gate 6, 15, 24, 33, 74, 80, 88, 89, 93, 98, 99, 100, 101, 102, 103, 106, 125, 129, 133, 136,
 137, 142, 147, 154, 142, 20, 154, 156, 164, 176, 187, 189, 194, 195, 196, 214, 226,
 227, 230, 232, 234, 239
 Gate maintenance 189
 Gates 10, 24, 72, 73, 81, 85, 125, 132, 194, 195, 234

Glass Break 77, 80, 231
Glass Break 23, 76, 101, 135, 231
Global Alarm Area 11, 84, 127
Graphics 4
Green Bar 64
Guard Booth 168, 171, 172, 173
Guard Tour 189

H

Hard Drive 4, 118, 120, 193, 228
Help v, vi, 1, 2, 7, 33, 47, 54, 61, 63, 64, 67, 77, 98, 100, 113, 124, 126, 130, 134, 139, 140, 146, 177, 179, 191, 192, 196, 198, 208, 212, 217, 227, 234
Hold Open 74, 88, 89, 93, 99, 100, 101, 102, 103
Hold Relay 74
Holidays iii, 9, 21, 23, 25, 65, 66, 139, 143, 144, 146, 206, 206
Home Office 24, 48, 51, 52, 53, 169, 170, 171, 172, 173, 234, 235
Host 4

I

Icons 27, 40, 41, 45, 54, 41, 67, 68, 229, 236, 239
ID viii, 6, 10, 18, 20, 22, 24, 78, 71, 80, 28, 80, 106, 120, 131, 134, 136, 197, 226, 232, 233, 234
If/Then 180
Ignore On-Site Activity 79, 210
Import 59, 109, 116, 117, 118, 120, 178, 212, 231
Inactive 218
Increment 189
Initial Database Setup 47, 48
Initialize Relays at Reset 132
Initial StorLogix Setup 47, 49, 57, 58
Initial TaskMaster Setup 218
Input viii, 18, 19, 23, 77, 89, 95, 23, 25, 77, 78, 80, 89, 102, 111, 20, 114, 116, 128, 135, 164, 167, 168, 169, 170, 171, 172, 173, 174, 175, 179, 188, 208, 229, 231, 237, 238
Input Points viii, 116
Inputs to Camera 20, 147
Inputs to Relays iv, 149, 164, 165
Inputs to Units iii, 109, 114, 115, 116, 117, 118, 119, 120, 200, 206, 212, 232
Input Tamper 77, 80, 231
Install 7, 27, 28, 30, 31, 32, 33, 34, 45, 202, 232
Installation v, 1, 2, 5, 22, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 47, 71, 80, 81, 92, 161, 191, 192, 199, 202, 214, 215, 224, 228, 231, 236
Installer 7, 28, 49, 200, 214, 215
Interface vii, viii, 6, 33, 41, 45, 149, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 229
Interface to Other Management Softwares 149
Interface to TaskMaster 149, 176
Internet vi, 4, 5, 6, 28, 169, 170, 171, 44, 55, 160, 171, 169, 172, 173, 174, 175, 201, 202, 203, 214, 217, 219, 221
Internet Information Services 161
Invalid Access Attempt 128, 136, 137, 232, 239
IP viii, 4, 6, 23, 25, 141, 147, 166, 167, 168, 169, 170, 171, 147, 20, 171, 172, 173, 174, 175, 202, 203, 229, 232, 236, 237

IT 4, 217, 218, 219, 220, 222, 223

K

Keyboard 4

Keypad vi, vii, 11, 13, 15, 22, 23, 81, 88, 90, 95, 98, 99, 103, 125, 126, 127, 128, 131, 132, 133, 134, 98, 134, 20, 134, 135, 136, 137, 142, 153, 154, 155, 156, 157, 159, 189, 195, 196, 227, 228, 229, 230, 232, 234, 235, 237, 239

Keypads 15, 22, 70, 106, 15, 90, 97, 98, 106, 120, 64, 125, 127, 131, 134, 135, 150, 154, 155, 157, 196, 226, 228, 229

Kiosk Module 217

L

Late Exit 133, 135, 136, 137, 210, 228, 231, 232, 233, 237

Late Fees 223

Law 217, 219, 220, 221, 222, 223

Legal 217, 219, 220, 221, 222, 223

License , 35, 230, 38, 45, 217, 220, 222, 223

License Agreement 217, 218, 220, 221, 222, 223

Licensing 42, 43, 45, 235

Lighting Areas iii, 9, 12, 13, 23, 25, 83, 87, 88, 89, 95, 100, 111, 112, 116, 117, 120, 129, 188, 208, 232, 234, 236

Lights 10, 12, 23, 24, 72, 83, 85, 88, 87, 89, 64, 89, 88, 95, 100, 111, 120, 125, 128, 129, 132, 164, 180, 186, 197, 232

Loading StorLogix iii, 27, 35

Local 48, 51, 67, 167, 168, 169, 170, 171, 172, 173, 174, 175, 178, 232

Lockdown 100, 106, 227

Logical Anti-Passback 133, 136, 232

Login 17, 36, 39, 50, 53, 55, 67, 227, 232

LogixScript ii, vi, viii, 9, 10, 25, 61, 72, 74, 75, 180, 81, 61, 85, 128, 180, 181, 186, 187, 188, 189, 239

LogixScript 'If' Functions 188

LogixScript 'Then' Functions 189

LogixServer iii, 27, 28, 38, 39, 40, 41, 45, 47, 51, 52, 55, 67, 167, 168, 169, 170, 171, 172, 173, 174, 175, 202, 203, 208, 212, 232

Logo 220

Log Off Time of Day 19, 23, 19, 23, 129, 136, 210, 232, 129, 136, 210, 232

Lost or stolen card 150, 151

M

Machine Key 44

Maintenance 218, 221

Malware 201

Management Interface vii, 6, 41, 167, 168, 169, 170, 171, 172, 173, 174, 175, 178, 179

Management Software vi, 6, 24, 33, 45, 176, 177, 229, 232

Manager 223

Manual trigger 74

Maximum AI Devices 131, 136, 232, 233

Maximum Code Size 131, 136, 210, 233

Maximum in Area 188

Maximum Users in Area 100, 106, 233

Memory 4

Menu Bar 54, 67, 150, 153, 162, 164, 167, 168, 169, 170, 171, 172, 173, 174, 175, 206, 208, 210, 212, 233
Message to Use Next 154, 156
Microsoft Windows ii, 4, 45, 28, 229
Modems 4, 217
Modules 217, 218
Momentary Off 189
Momentary On 183, 185, 189
Monitor 4
Monitoring 80, 85, 86, 166, 168, 171, 172, 173, 174, 231
Motion Sensor 77, 80, 233
Motion Sensors 23, 76, 77, 80, 89, 95, 101, 114, 120, 128, 135, 164, 231, 232, 237
Mouse 4
Move Out 218, 219, 220, 222
MSDE viii, 27, 29, 45, 233
Multiple Sites 3, 7, 24, 25, 48, 51, 52, 67, 140, 166, 170, 174, 235, 236
Multiplexer 10, 11, 22, 24, 71, 80, 134, 198, 226, 233
Mux 18, 20, 24, 115, 206, 210, 233
Mux and Channel 115, 206

N

Name 219
Navigation 47, 54, 221
Network iv, 23, 25, 48, 51, 52, 53, 55, 118, 141, 147, 149, 166, 177, 178, 203, 218, 219, 229, 232, 236, 237
Networking 141, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 203, 229
Networking StorLogix between a remote computer and multiple sites via the Internet 170
Networking StorLogix between Many Sites 174
Networking StorLogix between two computers 167
Networking StorLogix on multiple computers and a DVR via the Internet and a Router 173
Networking StorLogix on two computers and a DVR 168, 171, 172
Networking StorLogix on two computers and a DVR via the Internet 171, 172
Networking StorLogix on two computers and a DVR via the Internet and a Router 172
Networking StorLogix on two computers via the Internet 169
Networking StorLogix to a DVR 166
Networking StorLogix with a Central Corporate Server 175
Norton Anti-Virus® 5
Notice iv, 205, 214, 215 217, 220, 223
Notification 222
Nova 6, 24, 233, 234
Number of Uses Allowed 151
Numeric Value 185, 188

O

Off-Site 106, 120, 129, 184, 185, 189, 233
On-Site 2, 16, 24, 64, 79, 86, 89, 102, 103, 106, 107, 111, 120, 129, 133, 134, 162, 166, 180, 182, 184, 185, 188, 193, 208, 210, 215, 227, 233, 235
On During Time Schedule 89
Operators iii, 8, 17, 24, 50, 53, 54, 62, 67, 97, 104, 105, 106, 194, 234
Optional Setup iii, 139, 147
Other Setup iv, 149
Output viii, 11, 80, 234

Output Points viii
Owner 217

P

Paid To Date 221
Panic 75, 80, 86, 234
Panic Alarm 75, 80, 86, 164, 234
Pass Through Lighting Area 12, 89, 95, 234
Password 7, 17, 20, 36, 39, 50, 53, 67, 104, 105, 106, 141, 166, 168, 170, 171, 172, 173, 174, 175, 203, 208, 227, 232, 234
Paymentech 6, 24, 233, 234
PayXpress vi, 6, 24, 125, 127, 136, 176, 233, 234
pcAnywhere® 4, 5, 24, 221, 234
PDF 30, 45, 226, 234
Permanent 151
Points-of-sale 166, 168, 173
Poll Timeout 131, 136, 234
Ports 4, 24, 52, 167, 168, 169, 170, 171, 172, 173, 174, 175, 201, 202, 203, 236
Power 5, 25, 127, 136, 193, 234, 238
Pre-Installation Worksheet 1, 7
Preferences iii, 47, 55, 67, 74, 78, 86, 89, 100, 115, 126, 131, 234
Printer 4, 193
Processor 4
Product Overview vi
PTI Asia 225
PTI Australasia 225
PTI East 225
PTI Europe 225
PTI Integrated Systems World Headquarters 225
PTI Los Angeles Presentation Center 225
PTI UK 225

Q

Quick Help Bar 54, 67, 234

R

Radio frequency interference 197, 200
RAM 4
Rearm 18, 100, 106, 111, 112, 116, 117, 120, 208, 235, 236
Receipt 218, 221, 223
Red Letters Fields 49, 67, 235
Reference ID Fix 197
Refund 222
Region 7, 24, 58, 67, 235
Register 42, 43, 44, 45, 235
Registering the Software 27, 43
Registration 223
Relay 10, 11, 12, 20, 22, 23, 24, 70, 72, 73, 74, 75, 76, 80, 81, 84, 85, 86, 87, 88, 89, 92, 93, 95, 120, 124, 125, 128, 129, 132, 134, 136, 137, 142, 147, 154, 156, 164, 165, 180, 181, 183, 184, 185, 186, 188, 189, 195, 206, 208, 210, 226, 227, 228, 229, 230, 232, 233, 234, 235, 236, 239

Relay Board 10, 22, 24, 70, 81, 134, 226, 235
Relays to Camera 20, 147
Remote Assistance 4, 5, 24, 221, 235
Remote Computer 169, 170, 171, 172, 173, 174
Remote Device 206
Rent vi, 18, 24, 45, 206, 218, 219, 232
Renting 33, 151
Repeat Count 74, 81, 86, 235
Repeat this Message 154, 156
Report 79, 206, 212
Reports 7, 49, 53, 57, 61, 77, 206, 210, 212, 218
Request to Exit 128, 137, 235
Required Level On-Site 24, 102, 107, 235
Requirements iii, 1, 3, 4, 6, 219, 220
Reset 55, 132, 152, 186, 189, 210
Reset All Messages 55
Reset Bad Attempts 132
Resolution 4, 6
Restrict Access 63
Result File 179
RFI 197, 200
Router 172, 173, 174, 175
RS232 viii, 24, 52, 202, 208
RS485 viii, 131, 136, 197, 208, 234
Run 28, 45, 61, 167, 168, 169, 170, 171, 172, 173, 174, 175, 185, 189, 236

S

Script 61
Search vi, 113, 116, 120, 140, 142
Security Guard 168, 171, 172, 173
Security Levels iii, 8, 17, 24, 47, 59, 60, 61, 62, 67, 104, 107, 208, 212, 236
Send Alert 169, 189
Send All to Falcon XT 202, 212
Serial 24, 25, 28, 43, 44, 68, 202, 236, 238
Serial Number 43, 44
Serial Port 24, 202, 236
Server 28, 29, 39, 45, 167, 168, 169, 170, 171, 48, 171, 170, 172, 173, 174, 175, 203, 233
Setup 5
Setup Access Areas 97, 98, 99, 100, 101
Setup Access Levels 97, 102, 103
Setup AI Device Properties 124, 125, 126, 127, 128, 133, 136, 137, 232, 234, 237
Setup Alarm Zones 83, 84, 85, 86
Setup Alerts 60, 146, 162
Setup Buildings 83, 90, 91
Setup Cards 60, 150, 151, 152, 206, 210
Setup Custom Messages 60, 153, 154, 155, 156, 157
Setup Device Properties 123
Setup DVR 20, 139, 140, 141, 142
Setup Elevators 83, 92, 93, 94, 208
Setup Events to View 139, 145, 146, 147, 163, 239
Setup Falcon XT 19, 123, 129, 130, 131, 132, 133
Setup Holidays , 21, 139, 143, 144

Setup Inputs 69, 76, 77, 78, 79, 109, 114, 115, 116, 117, 118, 119, 164, 165
 Setup Inputs to Units 109, 114, 115, 116, 117, 118, 119
 Setup Lighting Areas 83, 87, 88, 89
 Setup LogixScript 181
 Setup Operators 17, 97, 104, 105
 Setup Relays 69, 72, 73, 74, 75
 Setup Screen 47, 50, 56, 57, 59, 62, 63, 66, 67, 70, 71, 72, 73, 76, 77, 84, 85, 87, 88, 90, 91,
 92, 94, 98, 99, 102, 103, 104, 105, 110, 114, 115, 124, 125, 129, 130, 140, 142, 143,
 144, 145, 146, 147, 149, 150, 151, 153, 159, 165, 163, 166, 168, 171, 172, 173, 174,
 175, 179, 197, 200, 206, 208, 210, 212, 230, 236
 Setup Units 18, 109, 110, 111, 112, 113, 116, 117, 120, 236
 Setup Wizards vii
 Shunt 80, 227
 Silence 75, 81, 86, 189, 236
 Silence Alarm 75, 81, 164, 189
 Silent Alarm 75, 86, 164
 Simple System Reset 193
 Sirens 11, 22, 24, 25, 55, 67, 72, 73, 83, 84, 85, 95, 100, 129, 227, 228, 230, 233, 236
 Site Code 7, 25, 54, 57, 67, 68, 170, 175, 236, 239
 Site Graphics 4, 99, 111, 132, 146, 208
 SMTP 161
 Software Activation 27, 44
 Software End User License Agreement 217
 Sounds 11, 22, 55, 67, 78, 80, 81, 84, 85, 86, 95, 111, 120, 127, 129, 145, 146, 147, 189, 227,
 228, 229, 230, 231, 233, 235, 236, 239
 Specifications 4
 Spyware 201
 SQL viii, 28, 29, 167, 168, 169, 170, 171, 45, 171, 170, 172, 173, 174, 175, 233
 Start Bar 28, 45, 236
 Stolen card 150
 Suggested Relay Time 73
 Support (See also Technical Support) 218, 220, 221, 222, 223
 Surge Protection 5, 25, 238
 Swinger Count 78
 Swinger Shutdown 78, 81, 210, 236
 Switch 22, 24, 75, 78, 79, 80, 81, 89, 95, 79, 81, 20, 127, 128, 135, 136, 143, 144, 164, 176,
 184, 196, 198, 227, 229, 231, 234, 235, 236, 239
 Switches 23, 77, 80, 81, 24, 72, 76, 77, 80, 101, 85, 25, 20, 114, 120, 135, 164, 199, 229,
 231, 232, 233, 234, 238
 System 217, 218, 221
 System Function 188
 System Requirements 4, 219, 220

T

Tailgating 126, 133, 134, 227
 Tamper 19, 23, 25, 76, 77, 80, 81, 127, 135, 208, 229, 231, 236, 238
 Task Area 54, 67, 236
 TaskMaster vi, 4, 6, 24, 33, 131, 41, 136, 149, 176, 177, 233, 234
 TCP/IP viii, 4, 25, 167, 168, 169, 170, 171, 172, 173, 174, 175, 202, 203, 236, 237
 Technical Support v, 2, 4, 24, 43, 44, 119, 129, 132, 166, 176, 177, 191, 193, 196, 198, 200,
 217, 218, 220, 221, 222, 223, 224, 225, 234, 235
 Temporary Internet files 201

Test Connection 48, 51
Timed - Counted Late Exit 133, 137, 237
Timed-Logical Anti-passback 133
Timed Anti-Passback 133, 137, 237
Timed Late Exit 133, 137, 237
Timed Operating Mode 126, 137, 237
Time of Day 19, 23, 129, 136, 182, 188, 210, 232
Timers 186, 188, 189
Time Schedules iii, vii, viii, 9, 12, 16, 21, 22, 25, 47, 63, 64, 65, 66, 68, 74, 87, 88, 89, 93,
99, 100, 101, 102, 103, 106, 133, 136, 143, 144, 147, 188, 206, 226, 233, 237
Time Slots (see also Time Spans) 9, 64, 65
Time Spans 64
Time Zones 52, 68, 206, 212, 237
To Access Area 135, 137, 231, 237
Tool Bar 54, 56, 68, 237
Trademarks ii, 220
Training v, vi, 2, 62
Transfer 218, 219, 220, 222
Transmitter 78
Transmitter ID 78
Trip on Input 89, 95, 237
Troubleshoot 92, 179, 196, 198, 203, 218
Troubleshooting iv, 23, 55, 129, 131, 132, 134, 145, 162, 179, 191, 192, 193, 194, 195, 196,
198, 200, 201, 202, 203, 214, 224, 228, 230
Troubleshooting Access Issues 191, 196
Troubleshooting Computer Issues 191, 201
Troubleshooting Concepts 191, 192
Troubleshooting Door Alarms and Inputs 191
Troubleshooting Gates 191, 194
Troubleshooting Network Issues 191
Turn Off 185, 189
Turn OFF to Activate 74, 81, 238
Turn On 184, 189

U

Uninterruptible Power Supply (See also UPS) 5, 25, 238
Unit iii, vi, vii, 9, 12, 18, 22, 23, 24, 25, 33, 45, 79, 87, 88, 89, 92, 95, 98, 99, 101, 103, 107,
109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 125, 130, 135, 141,
150, 176, 177, 188, 189, 198, 200, 206, 208, 210, 212, 225, 226, 227, 229, 230, 231,
232, 234, 235, 236, 238
Updates 5, 27, 28, 37, 40, 55, 61, 68, 201, 202, 217, 221, 222, 238
Upload 61
UPS 5, 25, 238
USB viii, 4, 25, 28, 52, 68, 201, 202, 238
USB Drivers 202
User iii, vii, 2, 6, 9, 12, 15, 16, 17, 20, 22, 23, 24, 25, 35, 36, 38, 39, 45, 53, 55, 60, 62, 63,
64, 66, 67, 77, 80, 87, 88, 89, 92, 93, 95, 97, 99, 100, 102, 103, 104, 105, 106, 107,
111, 120, 125, 126, 127, 128, 129, 130, 132, 133, 134, 135, 136, 137, 147, 149, 150,
151, 153, 154, 155, 156, 157, 158, 159, 162, 163, 166, 168, 170, 171, 172, 173, 174,
175, 180, 184, 185, 188, 189, 206, 208, 210, 212, 215, 217, 218, 219, 220, 222, 224,
226, 227, 228, 229, 230, 232, 233, 234, 235, 236, 237, 238, 239
User Custom Message 153, 156

V

Vacant Alarms 19, 25, 130, 208, 238
Valid Access Attempt 136, 137, 232, 239
Verification 219
Version 4, 6, 218, 222
Video vi, 6, 23, 25, 41, 139, 140, 147, 166, 167, 168, 170, 171, 169, 174, 175, 201, 172, 229,
171, 172, 201, 173, 236, 171, 229
VideoViewer 41, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175
View iii, 60, 61, 139, 145, 146, 147, 162, 163, 230, 239
Virtual Relay 69, 72, 75, 81, 85, 128, 136, 184, 185, 234, 235, 236, 239
Virus ii, 5, 25, 239
VP 129, 155, 157, 196

W

Warnings iv, 194, 195, 205, 214, 215
Warranty iv, 205, 221, 224
Web 217, 221
Website 221
Wiegand viii, 6, 10, 15, 22, 23, 70, 81, 90, 95, 106, 120, 125, 126, 127, 128, 134, 135, 136,
137, 196, 226, 229, 232, 234, 239
Window Bar 54, 68, 239
Windows 4, 217, 221
Wireless viii, 10, 78, 86, 129, 130, 131, 136, 162, 164, 203, 215, 234
Wizard 30, 35, 38, 45, 51, 52, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 70, 71, 72, 73, 74, 75, 76,
77, 78, 79, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 98, 99, 100, 101, 102, 103, 104,
105, 112, 110, 126, 127, 128, 129, 130, 131, 132, 133, 141, 142, 143, 144, 145, 146,
150, 151, 152, 153, 154, 155, 156, 114, 115, 157, 161, 158, 159, 161, 162, 163, 164,
165, 202, 208, 212, 113, 157, 115, 113, 116, 117, 118, 119, 124, 140, 125, 113, 125,
239, 111

Z

Zip Drive 4